UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CUSTOMER DATA SECURITY BREACH LITIGATION	Case 1:19-md-2915 July 12, 2021 10:08 a.m. Pages 1 - 231

TRANSCRIPT OF MOTIONS HEARING

BEFORE THE HONORABLE ANTHONY J. TRENGA

UNITED STATES DISTRICT COURT JUDGE

APPEARANCES:

FOR THE PLAINTIFFS:

NORMAN E. SIEGEL, ESQUIRE, *PRO HAC VICE*
LINDSAY TODD PERKINS, ESQUIRE, *PRO HAC VICE*
BARRETT J. VAHLE, ESQUIRE, *PRO HAC VICE*
JILLIAN R. DENT, ESQUIRE, *PRO HAC VICE*
STUEVE SIEGEL HANSON, LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7112

KAREN HANSON RIEBEL, ESQUIRE, *PRO HAC VICE*
LOCKRIDGE GRINDAL NAUEN, PLLP
100 Washington Avenue South, Suite 2200
Minneapolis, Minnesota 55401
(612) 339-6900

JOHN A. YANCHUNIS, SR., ESQUIRE, *PRO HAC VICE*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
Seventh Floor
201 North Franklin Street
Tampa, Florida 33602
(813) 223-5505

COMPUTERIZED TRANSCRIPTION OF STENOGRAPHIC NOTES

APPEARANCES CONTINUED:

FOR THE CAPITAL ONE DEFENDANTS:

DAVID L. BALSER, ESQUIRE, *PRO HAC VICE*
S. STEWART HASKINS, II, ESQUIRE, *PRO HAC VICE*
JOHN C. TORO, ESQUIRE, *PRO HAC VICE*
ROBERT GRIEST, ESQUIRE, *PRO HAC VICE*
PETER STARR, ESQUIRE, *PRO HAC VICE*
SUSAN M. CLARE, ESQUIRE, *PRO HAC VICE*
JULIA C. BARRETT, ESQUIRE, *PRO HAC VICE*
KING & SPALDING, LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309-3521
(404) 572-4824

MARY C. ZINSNER, ESQUIRE
TROUTMAN PEPPER HAMILTON SANDERS LLP
401 9th Street, N.W., Suite 1000
Washington, D.C. 20004
(202) 274-1932

ROBERT A. ANGLE, ESQUIRE
TIMOTHY J. ST. GEORGE, ESQUIRE
TROUTMAN PEPPER HAMILTON SANDERS LLP
1001 Haxall Point
Richmond, Virginia 23219
(804) 697-1200

FOR THE AMAZON DEFENDANTS:

ROBERT R. VIETH, ESQUIRE
HIRSCHLER FLEISCHER, PC
8270 Greensboro Drive, Suite 700
Tysons Corner, Virginia 22102
(703) 584-8900

TYLER G. NEWBY, ESQUIRE, *PRO HAC VICE*
FENWICK & WEST, LLP
555 California Street, 12th Floor
San Francisco, California 94104
(415) 875-2300

THE CLERK: Case No. 1:19-md-2915. *In re Capital One Customer Data Security Breach Litigation*.

Counsel, will you please note your appearances for the record.

MR. SIEGEL: Good morning, Your Honor. Norman Siegel, Stueve Siegel Hanson in Kansas City, co-lead plaintiffs' counsel. My colleagues from my firm this morning, Lindsay Todd Perkins, Jillian Dent, and Barry Vahle.

THE COURT: Good morning. Welcome.

MR. YANCHUNIS: Good morning, Your Honor. John Yanchunis, also co-lead counsel.

THE COURT: All right.

MS. RIEBEL: Karen Hanson Riebel, co-lead counsel for the plaintiffs. Good morning.

THE COURT: All right. Very good. Thank you.

Mr. Balser.

MR. BALSER: Good morning, Your Honor. David Balser of King & Spalding on behalf of Capital One. I've got with me at counsel table Robert Griest and Peter Starr of King & Spalding. Also, Mr. Robert Angle of Troutman Pepper. With us, and several of whom you will be hearing from over the next couple of days, are seated in the gallery. We've got Ms. Mary Zinsner,

also from Troutman Pepper, Susan Clare from King & Spalding, Julia Barrett from King & Spalding, John Toro from King & Spalding, and Stewart Haskins from King & Spalding. We have Tim St. George, also with us from Troutman Pepper. And from Capital One, we have Mr. Steve Otero, Mr. Nick Klaiber, Ms. Betsy Sochar, and Mr. Thomas Hall.

THE COURT: All right. Welcome to everyone.

MR. NEWBY: Good morning, Your Honor. Tyler Newby of Fenwick & West on behalf of the Amazon defendants.

THE COURT: All right. Welcome.

MR. VIETH: Good morning, Your Honor. Robert Vieth of Hirschler, also on behalf of Amazon.

THE COURT: All right. Welcome to everyone.

We're here on a number of motions. I've reviewed all of them, and I think it's been disseminated that I'd like to start with the class certification and also the subject matter jurisdiction issues. They're, obviously, separate motions, but they're centrally bound up with each other.

And in that regard, with respect to the presentation on the class certification motions, I would like for you to start with the standing issue, both under Rule 23 and also the Article III issue, as

we go forward.

All right. Mr. Siegel.

MR. SIEGEL: Thank you, Your Honor.

Your Honor, we have a PowerPoint to help guide us today. I'm not typically a fan, but given the number of issues, I thought we'd create one.

THE COURT: All right.

MR. SIEGEL: This is a good reason. We're starting with a jurisdictional question, which is not what I intended. But, obviously, we'll start there.

THE COURT: All right.

MR. SIEGEL: Would you like a paper copy as we go through today for reference?

THE COURT: Please, if you would.

MR. SIEGEL: Sure.

(Documents are passed up to the Court.)

MR. SIEGEL: So, Your Honor, as you noted -- may it please the Court, first of all. It's nice to be in court, and we appreciate the opportunity to be here maskless after the last 18 months of litigating this case.

As I'm sure Your Honor is aware, a lot of work has happened while we've all been basically --

THE COURT: Right.

MR. SIEGEL: -- under quarantine that has

allowed us to present this motion today. And we intend to walk through the evidence and the information that will guide the Court on these important decisions.

Your Honor wanted us to start with the Article III standing issues. So my colleague, Lindsay Perkins, is prepared to argue that, but I would like to start because I do think, as a certification issue, the Article III issues should be pretty basic. So let me start there. And if it pleases the Court, it's slide 81. If you will, just give me a second to skip ahead, and we'll get started.

THE COURT: Before you get into this -- and you may be getting into it -- give me your view procedurally how the Court should be dealing with the Article III standing issue. We're really dealing with a factual challenge to jurisdiction. We're beyond a facial pleading challenge, and the posture of the case is a little bit of a hybrid. In one hand, it's being presented -- I think you view it as almost in the nature of a summary judgment standard, which would basically put the burden on the plaintiff.

I mean, the defendants have essentially argued within the context of a summary judgment rubric a lack of evidence. The burden would be on the plaintiffs to come forward with sufficient evidence,

viewed most favorably to them, to create a factual issue, which is a different standard than an evidentiary hearing where the Court can weigh the evidence.

So how do you suggest the Court proceed?

MR. SIEGEL: I think our presentation guides and speaks to this point.

THE COURT: All right.

MR. SIEGEL: So let me dig in. If I haven't answered your question by the time I'm through, I know you'll ask again. I think I will.

Part of our anticipated presentation today, if the Court thinks that it's necessary, is a rather detailed factual recitation, but I think --

Let's just start off really, which I think is the Court's sort of preliminary threshold questions about jurisdiction. And I think Your Honor kind of characterized it as there's a direct Article III issue as it relates to class certification and then one about, well, they've also filed this motion that looks very much to us like a motion for summary judgment. And we believe there's many contested issues mixed up with that question.

So I think, as a threshold matter -- and this is slide 82 in front of you -- there are some important

sort of admissions or issues that are really not in play. So, first of all, Capital One does not dispute that the Court has subject matter jurisdiction over plaintiffs' claims for breach of express and implied contract and unjust enrichment.

THE COURT: Well, it reserved on those, as I understand it.

MR. SIEGEL: That's right. I mean, as far as what's before the Court as it relates to class certification, we don't think there's anything as it relates to an Article III matter that has not been effectively conceded for purposes of finding standing for class certification.

And there's a good reason for that. The law is well-established that a party to a breached contract has standing regardless of the merits of the alleged breach. Likewise, unjust enrichment is a traditional basis in American courts for standing, which is the test for whether a claim is justiciable in federal court.

So instead, we have this sort of piecemeal approach where Capital One claims the negligence claim and state statutory claims based on contested factual issues of what happened to the data, and that's really what this comes down to. We'll demonstrate, after the

Article III comments here, why this sort of threshold assumption or presentation that Capital One is trying to make -- I know the Court understands that the -- from the pleadings that we pled that this information was, in fact, exfiltrated.

Indeed, the discovery over the last 18 months has supported those very factual allegations which got us past the motion to dismiss. In other words, the evidence has matched our pleading with respect -- particularly to these questions about what happened to the data. At a minimum, we believe there's a factual dispute with respect to the specific issues that Capital One has raised.

THE COURT: Let me just make sure I understand your position. Given the two different standards, there's the evidentiary standard typically applicable to an Article III determination where the Court weighs the evidence and makes factual findings as to whether or not there's Article III standing. There's a summary judgment standard applicable to a merits decision.

And your view is that if there is a factual dispute under the summary judgment standard, the Court can't resolve the Article III issue, based on the evidentiary standard, by weighing evidence that

necessarily is a merits issue that has to be resolved by the ultimate fact finder? Is that --

MR. SIEGEL: That's exactly right. So this is *Kerns*. This is the Fourth Circuit case *Kerns*. When the jurisdictional facts and the facts central to a tort claim are inextricably intertwined, the trial court should ordinarily assume jurisdiction and proceed to the intertwined merits issues. So that would be --

It's not a question of whether we can come in the courthouse door. It's really not a question of whether the Court can certify a class. It's really the next question that comes after that about, okay, what are these contested factual presentations about Capital One's perspective. The genie is back in the bottle. The data didn't make it past Paige Thompson. And that's meaningful versus our position, which is that impacts perhaps some of our claims, not all of our claims.

But in any event, we have strong evidence that this information was -- we know it was exfiltrated. That's not contested because Ms. Thompson has it.

But we have lots of evidence about the risks, where that data could be, how it can be used to the harm of the plaintiff class. All of those are factual

issues that we believe are going to -- because they're contested are ultimately going to be determined by a jury at trial.

And so if you -- if the threshold question is if the Court finds the jurisdictional facts are intertwined with the merits, then the Court necessarily has to assume jurisdiction. And we think Capital One is inviting error to come up with a different result.

So the Fourth Circuit cases, *Kerns*, *Vuyyuru*, which is V-U-Y-Y-U-R-U, these are all cases cited in our papers. And, effectively, they are saying that we are missing an essential element of the claim, which, again, is a merits issue which must be determined as part of the merits, and the Court should assume jurisdiction.

And there's actually a very recent -- I'm going turn to slide 88 skipping ahead a few here. There's a very recent case called *Blackbaud, Inc., Customer Data Breach Litigation*. This is an opinion from the District of South Carolina decided on July 1. So just a couple of weeks ago. And it was a similar challenge there challenging the traceability premised on the cybersecurity firm's report concluding there was, quote, no evidence that plaintiffs' PII was on the dark web or being made -- being marketed for sale.

It's effectively the identical argument Capital One is making here, and the court said, Look, this is intertwined with the merits of the claim and the causation elements of plaintiffs' tort and, in that case, consumer protection claims and, therefore, said it's not appropriate for an Article III challenge. We think that's on all fours.

And, again, the idea that when -- if the Court determines, as I think it has to, that these challenges to Article III standing are intertwined with the merits, it has to assume jurisdiction. And from our perspective, the procedural question you asked is the Court can consider class certification, in our view should certify the class.

And I'll explain what I think the Court needs to find with respect to jurisdiction to certify a class, and then we can move on to the merits, which we know both Capital One, Amazon, and plaintiffs are eager to do. But that's the sequence.

And because that merits challenge, that causation challenge, they've moved for summary judgment and incorporated all of these same concepts. We've moved for summary judgment on the contract claim. Much of this is going to be factually disputed, we believe, through a trial, including this question about really

what is the risk, what is the function of the data distribution, how much does Capital One know and expect about this data, you know, and whether it matters if a jury or the Court finds it ended with the capture of Ms. Thompson.

We don't think that matters. It may matter to one component of our damages claim, the question of whether the class would need protection prospectively. But we think that's really a jury question.

And you will hear a lot about today, I suspect, tomorrow as well, this concept of one of the plaintiffs' damages theories of course, breach of contract, the plaintiff should be in the position they should have been in had Capital One complied with the contractual obligations to protect this data. It didn't. What is the traditional damage for that? Put the plaintiffs in the position they should have been in. That's this concept of the future value -- present value of future monitoring, and we believe that is a legitimate claim for damage.

That claim for damage might be in question if Capital One can show that that risk isn't sufficient enough to support a claim for that damage. You don't need monitoring because in Capital One's world, the genie is back in the bottle. There's no question that

nobody can get their hands on this information for purposes of harming the plaintiffs.

And we'll explain today why, we think, we have the better of that argument from a factual perspective, that those arguments that Capital One is making simply are not consistent with what we discovered over the last 18 months.

So let me just walk back a little bit on the jurisdictional question, and then I'll move on to the facts just to make sure I've touched all the bases that Your Honor inquired about.

So this is on slide 83, and this is really where we come from in terms of questions about jurisdiction. Can we be here presenting this motion for class certification, or are we off to state court with these claims? And unquestionably, we should be here.

And it's well settled. We know from *Hutton*, the Fourth Circuit case, of course, applying long Supreme Court jurisprudence, that the representative plaintiffs are named plaintiffs in the complaint representing the class have to meet the injury-in-fact requirement that there's a causal connection between the injury and defendant's conduct and the injuries likely to be redressable by a successful outcome in the

litigation.

And so we pled those facts. The Court has found those facts to be sufficient for purposes of the initial pleading, not in the context of Article III, but in asserting our claims. Examples are on slide 84 with respect to Plaintiff Zielicke, Plaintiff Gershen, Plaintiff Sharp with respect to actual fraud. Other plaintiffs allege fraud as well.

The Court concluded in the order on the motion to dismiss that plaintiffs suffered actual misuse of their PII -- that was the claim -- and the plausible inference that Thompson shared the information with others or enabled others to receive that information and plausibly connecting the data breach to plaintiffs' alleged injuries. This is page 28 of Your Honor's order.

This Court further held, based on these allegations, it is also plausibly alleged that there exists, beyond the speculative level, the imminent threat of identity theft.

This is exactly what *Hutton* said, in the context of standing, was sufficient. It's not different here at the class certification stage.

THE COURT: Right. Those were the allegations --

MR. SIEGEL: Those were the allegations.

THE COURT: -- which the Court accepted as true. Right.

MR. SIEGEL: Yes, those are the allegations.

THE COURT: And there were allegations that there was, in fact, fraud experienced by these plaintiffs that was traceable.

MR. SIEGEL: That's right. And so -- but those facts -- we believe the discovery has borne out those allegations, and we'll walk through that.

THE COURT: All right.

MR. SIEGEL: But the point is there's no question that these plaintiffs have suffered fraud. And the question is is it a different standard at class certification, or is it a question about the merits. And I think it's very important to keep in mind with respect to these allegations, there's no case out there, that we're aware of, that says, well, wait a minute. The class certification stage, that looks different.

And we'll explain how it doesn't matter because all plaintiffs and all class members plainly have standing. That's what I want to walk through with -- for Your Honor. Because this should not be an issue at the class certification stage. We believe

it's an Article III matter.

We can fight about what is a contested material fact for purposes of a Rule 56 motion. We think Your Honor is going to conclude that there are lots of contested material facts and that we'll end up with the folks in that box deciding yea or nay. But as it relates to this motion, we don't think it's well taken.

So, again, we will walk through. We're just sequencing a little different than we had intended, how we were intending to approach this, but we will walk through those facts. Then we can return to the standing if Your Honor still has questions.

And, look, as I said, we know -- as I mentioned earlier, to unpack this a little bit, this is slide 86 -- that the challenges at best only apply to predominance questions. Okay. So there might be a question -- they didn't present it this way, but if you were being charitable to Capital One here, the question of whether everybody was harmed in the same way for purposes of later establishing Article III standing or asserting the same claims or damage, those are predominance questions that could theoretically impact the Court's consideration of class certification but shouldn't in this case. Because the challenges that

the defendant is making here -- defendants, I should say, are challenging in the first instance the representative plaintiffs actual fraud, which is not asserted as a classwide injury.

And so, Your Honor, how we intend to try this case is we have -- and I'm going to go through these in detail, in *Comcast* level detail, the Supreme Court case that -- and you asked this question maybe a year ago: What damages attach to what claims? We're going to go through that in great detail so Your Honor is comfortable with what we're asserting and the basis for those claims. We are not -- the classwide claims and the classwide damages apply to all class members the same way, and we will walk through that in detail.

The second thing they're challenging, these mitigation costs of individual named representatives, likewise, they're not a classwide injury that plaintiffs are asserting.

And then sort of in the end here tossed in is this concept that the present value of future credit monitoring cannot apply based on *TransUnion*. That's the damage I mentioned earlier, again, based on a merits determination that this information cannot be out there suggesting that any further monitoring is necessary. So --

THE COURT: The mitigation damages really just is -- the appropriateness of that as an element of damages is tied, isn't it, inextricably to whether there's satisfied the injury-in-fact element? Because if there's no injury-in-fact, I guess it's *Ramirez* and others have said you can't establish injury by virtue of even reasonable efforts to mitigate what you perceive as a threat.

MR. SIEGEL: Not quite right on how this lines up with *Ramirez*. So let me walk through that.

THE COURT: All right.

MR. SIEGEL: Because *Ramirez* is a completely different case. *Ramirez*, as a threshold matter, right, is a statutory claim.

THE COURT: Right.

MR. SIEGEL: This is on slide --

THE COURT: The analysis is the same. It's the same elements of the Article III analysis, correct? Whether it's a statutory claim or a common-law claim, it still comes down to the three elements of injury-in-fact, traceability, and redressability.

MR. SIEGEL: That's right, but it's not as applied. Because in a common-law claim -- let's take the contract claim.

THE COURT: Right.

MR. SIEGEL: The contract claim, the common-law claim, it's assumed under the law that there is damage. All elements of the claim are met once the contract is breached. That's it.

THE COURT: Well, I'm not sure that's quite right, actually.

MR. SIEGEL: It is, and I'm happy to walk through the law here on that. Because we do think that what the Supreme Court of Virginia has said is that the claim is fully formed upon breach.

THE COURT: Isn't it an element that you need not only a contract and a material breach, you also need a consequential injury?

MR. SIEGEL: But the law assumes an injury. Even a nominal -- even a nominal one. So, for example, the statute of limitations starts clicking away upon breach, not upon injury. It's not -- a negligence claim would be different, Your Honor. A negligence claim --

THE COURT: Stick with the contract claim. I know it's not involved here, but I think we're going to end up getting to that eventually anyway.

MR. SIEGEL: We will. Let me walk --

THE COURT: Let me just throw out a question that I have.

MR. SIEGEL: Yeah.

THE COURT: That is, if, in fact, you're right that under Virginia common law a mere breach is sufficient *de facto* injury, that doesn't necessarily mean that it's sufficient Article III injury; does it?

MR. SIEGEL: We think it does, sure. The concept of injury is not one that you have to show I'm out a million dollars or I have this broken leg. The court implies in a common-law claim -- and again, there's no Supreme Court case. In fact, the Supreme Court has been very consistent about treating these statutory claims -- and this is what *TransUnion* talks about, that if Congress is going to go create a law that says if A and B happened, you're entitled to $1,000, then there needs to be something more than a risk of that harm.

So let's just use *TransUnion* as an example. Let's say there's roughly 8,000 of these folks that *TransUnion* has in their records that are labeled as potential terrorists and there's some number of those that have credit reports issued with that information on it. That's all that happens.

The court had no trouble finding that those people were injured for purposes of Article III. It was the people that *TransUnion* only had a record of.

They never communicated that information to anybody else, and there was a stipulation that said it's only the smaller group that actually credit reports issued that suffered injury.

THE COURT: Right.

MR. SIEGEL: But they had no trouble once that report is issued that there was injury. And in a breach of contract case, once you do have a breach, you also have an injury. We have significant claims for direct injury that --

THE COURT: But the thing about *Ramirez*, as I reflect on it in light of what I think are going to be some of the central arguments here, and that is why Article III standing in *Ramirez*, with respect to the people whose credit reports hadn't been yet distributed, was not a jury issue?

MR. SIEGEL: Oh, I think it was. I think that's what *Ramirez* was all about. There was a verdict that included those people.

THE COURT: No. But why the Supreme Court wouldn't say -- I think they even admitted this -- there may be a substantial future risk that if another creditor would request the credit report of somebody whose credit report hadn't yet been distributed, there's certainly a substantial threat that that might

happen. Therefore, it's a merits issue. It goes to the jury.

MR. SIEGEL: Well, it did go to the jury. And I think what the Supreme Court says is that plaintiffs failed in their proof with respect to that cohort. I think that's what -- I mean, we know from *Lujan* that Article III standing kind of moves along with the case.

THE COURT: Right.

MR. SIEGEL: Most of the law still says, at the class certification standpoint, you need one representative plaintiff that has standing. That's it. That's your Article III obligation, whether the claim is justiciable in federal court. That's it, and we think we have that without question.

THE COURT: All right.

MR. SIEGEL: What *Ramirez* ultimately said was it was a failure of proof. Remember, the parties had this stipulation that said, you know, we know with respect to this group, the information id out. But it was clear that the harm was -- there was no risk. There was no possibility of harm because the time period had closed when *TransUnion* took care of it. The Supreme Court said, look, it's not in the stipulation, and so we find that it's a failure of proof.

And I think the analogy at the oral argument that comes up in the opinion is a fairly good one that they talked about. You leave the courthouse. You're a quarter of a mile ahead of a drunk driver. You make it home, and you're safe in your house. Right. Okay. On the way home, were you at risk? Sure. But once you made it home and your car is in the garage and you're in the house, that's cabined. It's over. It's finite.

That what's they said also in the opinion. That's what the majority equated that cohort that did not have this information published. Again, held only at *TransUnion*, never distributed.

We have the exact opposite here with respect to that cohort. The plaintiffs here are like the cohort that the court found no trouble finding standing and affirmed the jury's verdict with respect to that group because here -- I mean, this is what Capital One is trying to argue is a merits issue. It's exactly why it should be done at trial.

Because Capital One is trying to say, as a matter of fact, we're going to show by a preponderance of the evidence that this evidence could not have made it past Paige Thompson under any circumstances and that when Paige Thompson was caught, it was in a box. And there's no holes that box. There's no mechanism for

any information to get out. And, therefore, the class is just like that cohort in *TransUnion* for which the court found ultimately --

THE COURT: So what are the facts that get you to the jury on these?

MR. SIEGEL: Yeah. Well, let's go there because that is what we think is sort of the critical nuts and bolts here.

And if I can back up a little bit and just wind up a little bit of the factual presentation.

THE COURT: All right.

MR. SIEGEL: Because I do think it offers some context to exactly that question, Judge. And I will move through the facts quickly -- because I know you know the background facts -- and focus on the exact question you just asked.

But let me start with what is an overview of what happened here. We know back in 2015 that Capital One began moving information to the cloud based on its cloud-first strategy. We'll present information about the known risks with that here momentarily.

But just with respect to the specifics, we know that in March of 2019, the attacker began scanning Capital One's assets. Now, that's exfiltration. So it immediately removes it from cases where, oh, the

information didn't make it out or there's no evidence of it. But they conceded that the information is out and it's out by a criminal hacker. That's on March 23, 2019.

And then there's this period of over four months where Ms. Thompson is publicizing the fact she has this data and, as we'll explain, threatening to release it, some of the information that you asked about.

Eventually, a white hat hacker tells Capital One that the AWS data was publicly available on GitHub, which is where she published instructions on how to repeat the breach. After an internal investigation, Capital One identified that they had been hacked, and eventually, Ms. Thompson was arrested.

So this ties, of course, directly to the claims. And I just want to run through this quickly because I do think this goes to the standing issue as well. Your Honor knows about the privacy notice, the promise to all applicants to keep this information safe and confidential, and that they employ security to prevent exactly what happened here. That's the promise -- they did that for everybody who applied for a credit card at Capital One -- applying to all customers, applicants, and former customers.

Then we also know that with this migration to the cloud, that Capital One was one of the first major banks to do it. I know you know this from our arguments last year on the motion to dismiss. But Capital One made decisions about that. It retained this data indefinitely, even for applicants who had no credit card with Capital One. And it was stored on the cloud for both Capital One's benefit, but also Amazon's benefit.

So when they did all this, they did it with these known vulnerabilities. The way we look at this -- and I think in answering Your Honor's question, how will this unfold to a jury, well, let's talk about what was happening before the breach. When they moved this information, what were the risks they were putting everybody at? What did they know at the time?

There was the ModSec WAF. I know that's a term Your Honor recalls, the ModSec WAF. It was set to on. It should have been switched to off. They were supposed to check it quarterly. They never did, and it sat that way for four years. Once they started their migration to the cloud, they did not bother to go back and check the misconfiguration.

In fact, it was discovered prior to the breach, and we know that, too. We're on slide 14.

Different groups within Capital One noticed this setting was incorrect. Some fixed it. But then complaints to cyber effectively went unanswered, and they went unanswered because they were transitioning to another product, a Barracuda product. But that was never implemented before the breach after months and months or years of delay.

We also know about this SSRF forgery attack and how that could be used to capture this information from the AWS cloud, this Capital One data. They identified that threat. We have documents at least as far back as August 2018. That's on slide 15.

They also knew their roles, their permissions. Recall this fact, that part of the problem, part of what Ms. Thompson compromised were overpermission roles allowing her not just to look at this data for this purpose. But once she was in there, she could look at the entire dataset, and that's how she was able to extract what is equivalent to about a billion pages of documents involving nearly 100 million Capital One customers. So this is AWS explaining how Thompson accessed and used these overpermission roles to complete the breach.

In January '19 -- still pre-breach -- they identify a number of weaknesses that have been

identified as part of the penetration testing and, again, identify the need to further restrict access privileges, including enforcement of the principle of least access, which our experts talk about in detail, within the environment. They failed to do it.

Then, finally, there was a problem of detection. Again, this is a major evidentiary point that, I think, addresses Your Honor's question.

MR. BALSER: Your Honor, if I may. I'm sorry to interrupt Mr. Siegel. Before the hearing, I had identified to Mr. Siegel 12 documents out of the 350,000-some-odd documents that have been produced in the case as being particularly sensitive and documents that are under seal and subject to the protective order. Because I believe we have an open line here --

THE COURT: Yes.

MR. BALSER: -- I wanted to be vigilant with respect to those documents to the extent they were going to be introduced. This is one of them.

What I would suggest, if it's appropriate in Your Honor's view, is that we come to sidebar and discuss these with a sound muffler or otherwise just mute the public line while just these very few handful of highly sensitive documents are publicly aired.

THE COURT: All right. Are you going to get

into the substance of these at all?

MR. SIEGEL: A little bit, Your Honor, because they go directly to the question you asked. So I think we have to. I mean, from our perspective, it's an open hearing, but we'll do whatever the Court wants. We're not trying to --

THE COURT: These documents are under seal?

MR. BALSER: They are.

MR. SIEGEL: They are, Judge.

THE COURT: All right. I don't know if we can mute the public line.

We can?

THE CLERK: Yes, sir.

THE COURT: All right. Let's mute the public line for this purpose.

MR. BALSER: Thank you, Your Honor.

MR. SIEGEL: I think I know when it stops, but I'll get the high sign from Mr. Balser before --

THE COURT: All right. You are comfortable with everyone in the courtroom?

MR. SIEGEL: Your Honor, we believe there may be some press in the courtroom.

THE COURT: All right. Let's do it at the sidebar then. Let's go back and open up the public line.

(Under seal bench conference under separate cover.)

THE COURT: All right.

MR. SIEGEL: Your Honor, I do want to talk about some of the additional technical vulnerabilities and how those were really a function of what were significant problems at Capital One with respect to their cybersecurity risk management.

Slide 22, again, in April of 2019. So by this date, you'll recall from the time line, Ms. Thompson has exfiltrated the data of the class, the 98 million class members, and Mr. Holmgren, who is vice president for cybersecurity risk management and interim chief cyber risk officer, drafts this memo to the risk committee of the board of directors.

And keep in mind, Capital One is completely oblivious that Ms. Thompson has exfiltrated all of this information.

And among other things, Mr. Holmgren here is identifying the number of high-severity security vulnerabilities for externally-facing applications within the system noting that 81 percent or 1,331 being past due. It's really one of many documents in the record showing unresolved issues across its systems that were not timely fixed.

I will skip over 23 and 24, which we discussed at the bench, and move to 25, and this is now post-discovery.

And, Judge, again, in terms of what a jury will hear with respect to this question of what happened to the data, in large part, comes from Capital One's own documents. So, for example, we have Mr. Shultz, Christopher Shultz here, communicating on July 23, 2019. His is the director of cloud engineering. He says in talking about the breach: So bad proactive scanning, bad CSOC -- which is the cybersecurity operation center response -- bad perimeter management and a bad response purged the data events records making it more difficult to assess. I'm not finding anything they've done right.

Kyle Busekist, B-U-S-E-K-I-S-T, a lead software engineer responds: They saved money.

And that is indeed what Anthony Johnson, who is the former managing vice president of cybersecurity, testified in his deposition, that Capital One placed profit over consumer protection.

And, again, the lead-in as to what was going on when they -- they wanted to be at the head of the curve in the banking industry of moving to the cloud. When they presented their efforts to move to the cloud

at an AWS conference back in 2015, they said, you know, we're not going to do it by sending a little bit of data and trying to attack little problems. We're going to send all the data and try to attack the big problems.

But they just did it without the adequate protections in place, which unfortunately were brought to bear and resulted in this breach.

Let me touch on AWS and what they knew, and then we'll get into a little more of the specifics on the exfiltration issues. AWS knew as early as 2017 of the forgery attack vulnerability that was exploited in the breach. They knew that Capital One could not figure out that they were struggling with how to permission these roles, these access roles, and did not take action until after the breach.

And Your Honor knows from the order on the motion to dismiss the guard duty problems, its gap in coverage, including in Stockholm where the breach of data is believed to have come from. So they jointly worked on these efforts to protect the data. They know it's an issue, and they fail and fail miserably.

So they also both knew -- this is both Amazon and Capital One -- that these Amazon buckets, these simple storage solution buckets accessed by Thompson

were Internet accessible. In other words, it was not a situation where you have to be a Capital One employee trying to access the data from a Capital One computer. Anybody with an Internet connection could access this data.

We also know that there were many opportunities to timely discover the breach, and we talked a little bit -- there was at least three, and the first one in detail is on slide 32. Mr. Hopkins -- this is in a chat post-breach July 23 talking with Devon Rollins, the senior director of cyber intelligence. Mr. Hopkins, who was the director of cyber intelligence -- Mr. Hopkins says, there were so many lessons learned. I am devastated that CSOC didn't escalate the alerts. They were so critical and obvious in hindsight.

In other words, it was obvious that they had alerts that they didn't act on that would have flagged this breach in process and immediately after, none of which were followed.

And then Capital One engaged KPMG to do a risk assessment of the Cybersecurity Operations Center that Mr. Hopkins was referring to. So again, post-breach, December '19, backward looking, and KPMG identifies the Cybersecurity Operations Center, which,

again, is tasked with identifying these alerts, which misdiagnosed the alerts that related to the data breach and found deficiencies across people, processes, and technology. I won't read all of these.

I'll point you to a couple, Your Honor. With respect to people, KPMG found that the CSOC lacked sufficient staffing, resources, and technical expertise to execute its core responsibilities. With respect to processes, KPMG identifies that there were gaps in the intake process for threat information and undefined excalation procedures. They found that -- the third bullet point -- alerts are not regularly reviewed or updated for continued relevance or enriched with the most current threat indicators. And with respect to technology, KPMG reported that the Cybersecurity Operations Center lacks comprehensive visibility into potential threats throughout the enterprise due to the lack of consolidation logging from all security information and event management tools and the lack of deployment of decryption capabilities and gaps in cloud.

So, again, Capital One promises to protect all this data, and this is what's going on. In fact, once they promised to protect the data, we also know that Amazon had an opportunity to -- at least two

opportunities to detect the breach. First, in May 2019, someone passed an Amazon employee a note at a conference -- there's a picture there on slide 36 -- and it stated that Capital One had an open SOCKS proxy and identified the IP address.

This note was passed along to Capital One, but there's no indication anywhere in the record that any action was taken on this at the time.

Amazon also employed what are known as honeypots, Your Honor. These are sort of efforts to create false targets. In April 2019, that, in fact, detected an attacker who was performing the same activity as Paige Thompson on AWS cloud products. AWS did not notify its customers of this threat, including Capital One. It, obviously, would have shortened the time, at least, that all of this information was publicly available, including instructions on how to repeat Ms. Thompson's efforts.

So let me skip ahead, Your Honor, because a new document that was the source of significant litigation in front of Judge Anderson came to light in the discovery process that we think does several things with respect to liability. We think this is a key document in the case and are sort of flagging it for you for that purpose, and I'd like to go through it in

some detail.

So this is the Office of the Comptroller of the Currency findings with respect to the data breach. It's attached to our motion at Exhibit 14. This, we believe, will be admissible at trial. I don't think that's a determination the Court needs to make now, but it is plainly a record of a public office in a civil case and factual findings from an authorized investigation under 803(8)(A)(iii). There are other hearsay exceptions we think apply to this document. Again, it's not a determination the Court needs to make now, but I do think, when Your Honor asked about evidence, this is an important place to start.

So this is the supervisory letter that the OCC sent to Capital One following the breach. On slide 42 is the first conclusion offered by the OCC, and that is that the overall quality and effectiveness of Capital One's cloud operations are weak.

Moving on from there, management's ability to identify and appropriately manage technology and cybersecurity risks is ineffective. Weaknesses were identified across all three lines of defense, including governance and oversight, first and second line risk management, network configuration, and asset management processes, security processes, and internal audit.

They go on from there that the OCC identified foundational technology and cybersecurity weaknesses and control breakdowns within cloud operations that contributed to the data breach, concluding that during this incident, an attacker was able to penetrate Capital One's cloud environment undetected on several occasions and downloaded sensitive credit card application data from cloud storage buckets housed at Amazon Web Services on over 100 million customers in the United States and Canada. That's the first conclusion of several, Your Honor.

The OCC goes on, in their second conclusion, that the governance and oversight of cloud operations are weak. Management had several warning indicators from both internal and external sources that risk management activities needed improvements prior to the cybersecurity incident.

Again, the case is premised --

MR. BALSER: Your Honor, I'm sorry to interrupt. This is a document that's under seal and also should not be exposed publicly. I apologize for not having flagged it.

THE COURT: All right. You can refer me to the page. I can look at it.

This is their assessment as of December 2019;

is that right?

MR. SIEGEL: It is.

THE COURT: All right.

MR. SIEGEL: Your Honor, I would like to --

THE COURT: You've underlined what I think you're reading.

MR. SIEGEL: I've underlined the headlines of those conclusions.

THE COURT: Yes, and the Court has this and will review it.

MR. SIEGEL: So, Your Honor, while we're here then, I'll just submit the PowerPoint as an exhibit to the argument so it's in the record and there's no dispute about that.

THE COURT: All right. Some of the slides will have to be redacted.

MR. SIEGEL: It can be under seal.

THE COURT: All right. That's fine.

MR. SIEGEL: I would like an intact version of it as part of the record, and I have no objection to the entire thing being under seal until otherwise directed.

THE COURT: All right. Then portions can be unsealed.

MR. SIEGEL: Yes, Your Honor.

THE COURT: All right.

MR. SIEGEL: So I'll just refer to them by number then, Your Honor.

THE COURT: All right.

MR. SIEGEL: So Conclusion 3, obviously, we've underlined the headline to this particular portion. But it's important, we think, to read each and every paragraph here. Because, again, we think this is exactly what the jury is going to hear about Capital One's conduct and whether they personally breached the contract; whether they breached their independent duty, pursuant to our negligence claim, to protect this information; and with respect to those negligence claims, whether punitive damages are appropriate. It's a claim in the case, and we think this is a key document that supports it.

THE COURT: All right.

MR. SIEGEL: Conclusion 4: Again, you can read, and we ask the Court to do that.

Conclusion 5, Conclusion 6, Conclusion 7, I think, is particularly important, Your Honor. This is a finding that Your Honor can read. It is underlined, and I will effort not to disclose the contents of it. But it is an important issue in the case.

One of the questions, of course, in the case,

that is discussed in expert testimony. Okay. What does it mean when you say that you're going to follow federal law in the privacy notice? That is one of the things that Capital One is promising to do. We promise to follow federal law. That is their contractual obligation in the privacy notice, and the OCC's Conclusion No. 7 addresses that.

THE COURT: All right.

MR. SIEGEL: And then, Your Honor, this is perhaps the key point: At the end of the day, as reflected in this letter, on page 50, there is, obviously, what we view as a significant admission. Your Honor can read it. But the senior management from Capital One participated in the exit meeting where these conclusions were communicated to Capital One. You see there's all the key folks there related to cybersecurity, internal audit folks, corporate secretary, chief information officer, the interim chief information security officer, the chief risk officer. You can read the underlined statement in this OCC letter.

So look, again, as back to the threshold question what is the jury going to hear and what are they going to see, it's this. And if the question is did Capital One breach its contractual obligations, did

Capital One breach a duty, an independent duty to protect this information, this information -- to, I think, answer your question that you asked at bar a little further, the reason we think this is so important and the reason we're presenting it as part of class certification, this applies to 98 million people all the same way.

There is nothing in anything I've showed you related to what Capital One knew before the incident, while it was happening, what they said afterwards about how bad they were before, none of that impacts class members differently based on any criteria whatsoever. All of these documents apply to everybody the same way, and that is really the touchstone of what a class action is: Is the evidence going to be presented in a way that is universal to the class. And we think absolutely it is.

And thank you for indulging me for going through some of those facts.

THE COURT: All right.

MR. SIEGEL: So finally, where does this end up? It ends up with the identification of those failures of Capital One's management and board, the OCC, and the Federal Reserve Board levied an $80 million fine against Capital One and issued related

consent orders.

So let's talk a little about the impact of that. We talked about just the numerical impact across the class of what data was compromised at the bench. Slide 54, this is an internal summary of what was exfiltrated, and this is important for several reasons. First of all, 54 shows this, again, Capital One's Project Star report post-breach. It identifies exactly what was exfiltrated, and it identifies that it's in easy-to-use data formats and that it can be used to build customer profiles.

In other words, the different exfiltrated dataset -- and our expert talks about this -- can be used to collect data and create profiles about a single person, typically through an account ID. So an account ID might have a piece of data in one dataset. That same account ID linked to your name, Your Honor, would be searched in these other databases. You would build a profile for Your Honor's name across those databases.

And so the other important point of this data and the data on the previous slide that I identified for Your Honor at the bench is that we can slice and dice the data any way we need to ensure that the class -- if there's some claim that is truncated for some reason or we get to a point in the case where

there's an issue about, well, this person ended up with a card and these people didn't, we know exactly who those people are.

And so there's this concept often overused of ascertainability in class action litigation. But the real question is: Do you know who these people are? Can you identify them based on objective criteria? And the answer is yes.

And we know that from the way these datasets were not only comprised but the way they were held by Capital One. Again, our expert looked at the datasets, actually found some additional information that Capital One had not. But in any event, it's all there. It's all objective, all ascertainable.

The next slide I've talked about really already. This is Kevin Mitnick. I know you will hear a lot about Kevin Mitnick tomorrow. Mr. Mitnick looked at the dataset. He confirmed the data that Capital One identified in their interrogatory response. He identified these essential building blocks and how they could be built upon by comparing these databases. He confirms in detail that this is exactly the kind of data fraudsters would use to commit exactly the kind of fraud suffered by our plaintiffs and how that data can be internally enriched from those datasets but also

externally enriched. And, again, I know that's the subject of a motion in limine, which we'll take up tomorrow.

And this brings me, Judge, finally, to perhaps the question you asked 30 minutes ago, which is what do we know about exfiltration. So we know about what we view as very bad conduct that would support a claim of punitive damages in this case with respect to a negligence claim, that those facts apply to everybody the same way. The question you asked, you know, is this data exfiltrated, and we do know it was exfiltrated. It was exfiltrated by a hacker as a result of the defendants' negligence.

Again, this question about whether Capital One is going to be able to prove it can put the horse back in the barn or the genie back in the bottle or whatever analogy you want to use, we're skeptical and believe it's a deeply disputed factual issue.

But, again -- I mentioned this in the first few minutes of the discussion -- if this is something that Capital One ultimately can prove, it impacts one claim of damage, and that is whether this class needs to have monitoring going forward. If Capital One can prove this data is not out there, there is no risk to anybody anymore because the genie is back in the

bottle, the horse is back in the barn, then, sure, they may be able to make a case that we don't need prospective monitoring.

But all the other claims survive, and I'll talk about the damages at some length as we move forward here. But what we characterize as the license value for the PII survives. The disgorgement for unjust enrichment survives, and of course, the alternative claim for nominal damages survive.

I mentioned briefly at the bench that there are well-worn concepts at common law about, okay, what happens -- you know, Capital One has said, well, how do you even know that this fraud that your representative plaintiff had was the result of our breach? There's been a lot of breaches. That's another sort of collateral attack, but it's one that Virginia law speaks to about what happens when there's a single injury but perhaps multiple causes, multiple negligent acts, some of whom you may know, some of who you may not know, and the concepts of concurring negligence.

We've put some significant thought into a trial plan for this case, Judge, and there's little doubt that under Virginia law, which will apply here, under these concepts of negligence, that it's going to be up to the jury to determine whether there's a

sufficient indication that Capital One is responsible. Then it's Capital One's responsibility to say, We're not.

And this was addressed, actually, in a data breach case -- the next slide -- a Seventh Circuit Case. It took up the question in the *Neiman Marcus* case about -- the defendant was raising this precise issue that, well, wait a minute. There's all kinds of breaches.

I think you know: Mr. Balser and I worked together on the *Equifax* case on opposite sides. They have mentioned that case. They mentioned other breaches. But if there are multiple companies that could have exposed the plaintiff's private information to the hackers, then the common law of torts has long shifted the burden of proof to defendants to prove that their negligent actions were not the but-for cause of the plaintiff's injury. It is very much a jury question. And how ultimately those burdens play out at trial, obviously, will be the subject, I suspect, of much.

THE COURT: I think there was a first year torts class on this issue, who shot the gun.

MR. SIEGEL: I suspect we'll have lots of briefing about who shot the gun between now and trial,

Judge.

But conceptually, these are issues that -- I think the jury is going to be instructed. We'll figure it out. But these concepts of, well, you know, having established definitively that this information was out, that it was hacked, you know, what comes next and what the impact of that is we believe are all jury instructions. And I suspect we'll have an opportunity to brief at length what those instructions should look like.

So let's look at what Capital One is saying about this exfiltration because this is really the basis of the question you asked. What they've incorporated into the class certification process is this idea that the genie is back in the bottle, and they point primarily to what the government said in a criminal case. That's what they're pointing to.

They have an internal document where they do a sort of psychoanalysis of Paige Thompson, and they're like, well, you know, based on that -- they call it a theory, and then they have this, which is the criminal complaint and what the DOJ has done in a criminal case about what charging decisions they're making under a different proof standard in a criminal case. That's what Capital One is presenting to this Court to make a

finding to cut off liability in this case.

And the way the government characterized it was, quote, We believe and hope we have recovered the stolen data in the case. We believe and hope.

In the same filing, they say, Regardless of what Thompson might promise to the Court, she previously threatened to disseminate stolen data containing tens of millions of people's personal identifying information. Again, this question of further exfiltration, whether other people could have had it, it's very much a disputed issue.

And again, just even looking at Capital One's own documents, the first one I'll show you on slide 61. This is part of the Project Star evidence. She publicly shared the information for how to access the data. We've explained that in our papers, but this is Capital One describing how this information was available on Twitter, how she posted it to GitHub providing the keys, if you will, to this Capital One data that was available for anybody to access.

On the next slide, this is the hacker herself. This is what she's saying publicly and what the jury will see, and the jury will decide whether there's additional exfiltration. I want to get it off my server. That's why I'm archiving all of this. So

erratic is Ms. Thompson. That's a stipulated fact in the case. So she's communicating with other people publicly and publicly stating that she wants it off her server and is archiving the information.

Slide 63, she says, I am going to give this all to this desperate Chinese dude who scams people. Again, a statement by the hacker indicating that she's going to distribute the data.

The next slide, a Twitter post. All of this is public by the way, none of which Capital One saw. This is in June, a month before they discovered the breach. She's posting on Twitter: I want to distribute those buckets, the data. There are social security numbers with full name and date of birth.

Let's look at what Capital One's view of it was in slide 65. This is Houston Hopkins again, the director of cyber threat management. So this is Capital One's view of it: I am worried she has bundled away somewhere that it will be waiting for her when she gets out. I am worried that she has this bundled away somewhere that it will be waiting for her when she gets out.

And Anna McAbee responds -- she's an associate, now works at AWS -- yep, same. I bet she has it hidden somewhere good.

This is Capital One contemporaneously expressing they're willing to bet on it, right, that she has stored this information away and will use it for ill once she's out of prison.

Finally, I just want to point to the superseding indictment, not because I think it's particularly relevant or admissible in any way because it's not. The government recently did add Count 9 saying that Paige Thompson attempted to use personal identifying information, including more than 15 social security numbers and more than 15 bank account numbers stolen during the conduct described in Count 1 to create counterfeit and unauthorized credit and debit cards to be used to conduct transactions in interstate and foreign commerce.

So Capital One used that initial criminal complaint that was superseded in June, which now has this claim. The No. 15 is statutory as a part of that statute, Judge. It's not an indication. It's only 15. So now the government is even saying that Thompson expressly was using this information for identity theft and fraud to the extent that is relevant at all.

The next sort of significant piece that I touched on earlier was the fact that -- and what the jury is going to hear is how do we know. Well,

typically, the way you know is that there are very strict logging requirements that anybody who is promising to protect data, anybody who has a duty to protect data would log what is being accessed to their system.

So on slide 67, we know that Capital One deleted critical logs, in violation of its own information security standards, and that very few logs were available for the post-breach investigation. So we know post-breach that Mandiant requested certain logs so they could try and figure out what exactly happened, whether there were other attackers. There were three logs that they asked for that Capital One could not produce, the Apache Web Services events logs, the Web Application Firewall event logs, and the Elastic Load Balancer event logs.

This is the mechanism by which Ms. Thompson exfiltrated 98 million customers' information, and they didn't maintain any logs. They can't prove that the stuff is not further out there, and we think the weight of the evidence suggests that it very, very much is.

These logs were deleted in 7 or 30 days when their policy indicated they should have been maintained for at least 120 days, if not 13 months.

Mr. Stuart Madnick, his seventh opinion here

goes through this in detail. And just incredibly, Michael Johnson, who was the chief information security officer, knew that they were not maintaining these logs and nevertheless -- he issued a memo about it. It's cited in our papers, and Dr. Madnick discusses it. He identified that we're not maintaining logs pre-breach; yet, nobody did anything about it.

And so post breach, to answer Your Honor's question is Capital One going to be able to prove that this information isn't well past Paige Thompson, we think not.

So what do we have? We have the discarded logs which were the ones requested by Mandiant that would have detected additional malicious activity. Those are gone. The available logs would not have captured the breach activity under certain circumstances either, and that is explained as well by Dr. Madnick.

The testimony on the next slide from Michael Hedrick explains that even on the logs they had, they could not tell under certain circumstances whether there was additional attacks of exfiltration. And remember, during this entire time period, they weren't maintaining logs, and they can't track it through the logs they did keep, the cloud trail logs. This

information is publicly available to the world, and Ms. Thompson is aggressively promoting the fact that she stole this information from Capital One.

So as a final point on this, Your Honor -- because it goes to part of our theory of the case and damages -- how did they respond in addition to betting that she has it squirreled away somewhere good and all the other missions we went through? They offer credit monitoring. This is Capital One acknowledging the risk and the remedy to address that risk.

They are telling people in this notice post-breach to beware: You are at risk. They are offering credit monitoring. Why are they offering credit monitoring? Because they promised to keep the data secure, and they didn't. And it's appropriate to offer that, but as a remedy to a breach, it's also appropriate.

Finally, Your Honor, we know that as late as February 2021, they were still taking the same position. They say, We think it's not out there. But in this letter just uncovered in Maine, they are still saying, We're offering credit monitoring.

And, again, it's just not consistent to say on the one hand you're not at risk, we can guarantee this information is secure, and on the other hand say

here's credit monitoring and you are at risk.

Your Honor, I am at a good stopping point if it's appropriate to take a short recess. I can keep plowing ahead too if that's your preference.

THE COURT: That's fine.

Let me just summarize what I understand you're saying. Again, I'm still focused on the Article III issue, and the issue is whether there's sufficient injury-in-fact that's concrete and particularized and is either actual or imminent.

As I understand your position -- and this is a case where I think we're in agreement -- there's no affirmative action that any of these named plaintiffs at least or really anyone can actually point to any actual use of their personal identification that's traceable to this breach.

MR. SIEGEL: I'll stop you there. We disagree.

THE COURT: All right.

MR. SIEGEL: We disagree. So we've identified more than a half a dozen plaintiffs that had fraud following the breach that our expert says used information that was compromised in the data breach. Is it the same information?

THE COURT: Well, that's the issue. It has

to be traceable.

MR. SIEGEL: Of course it does.

THE COURT: Right.

MR. SIEGEL: But it doesn't have to be traceable from a criminal standpoint. I mean, look at *Hutton*.

THE COURT: I want to hear more about that, but let me just summarize what I was going to say. That is, as I understand your position, this imminent actual injury can be reasonably inferred by a fact finder --

MR. SIEGEL: Yes.

THE COURT: -- based on the pre-breach vulnerabilities that created the possibility of not only what actually happened but other hackers, the fact that anyone with an Internet connection could access the data that was exfiltrated from Capital One because of these vulnerabilities, Thompson's own declared intentions and her own advertising of the data, the post-breach vulnerabilities that were assessed as of December 2019 at least, the nature of the data that was exfiltrated that made it possible to use the data in a way to create IDs, and Capital One's own inability to establish that there was anyone else that hacked it or that it has been sufficiently contained.

MR. SIEGEL: I think that's a fair summary.

I would just conclude with going back to *Hutton v. NBO*, a case Ms. Perkins and I litigated through the Fourth Circuit after we were dismissed for lack of Article III standing. Because there NBO denied they were even the victims of a breach.

THE COURT: Right, I understand. And then you want to add to that specific instances where post-breach some of these named plaintiffs actually experienced use of their personal identification, admittedly, without the ability to say where it came from.

MR. SIEGEL: That's right, and what our expert says it is the type of fraud you would expect to see following this kind of breach, right. I mean, it is not can you follow a piece of data out of Capital One into a hacker, Paige Thompson or somebody else, into another hacker that committed fraud on our named plaintiffs? The answer to that is no, but that's not the standard.

THE COURT: All right.

MR. SIEGEL: That's not the standard.

I do think *Hutton* is instructive here because, again, there you had a defendant who said, We were not even breached. It's not our data.

And yet, what the Fourth Circuit says is, Well, these people did suffer fraud, as ours have, and it's reasonably correlated to the data that was compromised in that breach, Article III standing.

And that standard is not different at class certification. It's not.

THE COURT: All right.

MR. SIEGEL: So that's the basic threshold question with respect to the representative plaintiffs.

THE COURT: All right. Why don't we take a 15-minute recess.

MR. SIEGEL: Thank you.

MR. BALSER: Your Honor?

THE COURT: Yes.

MR. BALSER: Would it be helpful for the Court to have me respond to the standing arguments before Mr. Siegel gets --

THE COURT: I'm thinking about that. What other piece do you want to move into, Mr. Siegel?

MR. SIEGEL: The class certification elements.

THE COURT: All right. Let's continue with you and then --

MR. SIEGEL: I think we've covered most of the facts. I think now we're into here's what we want

certified and why, and I do want to walk the Court through damages and make sure that you understand. You've asked us before, so I want to make sure we address it with sufficient specificity, the damages we are claiming with respect to each claim in the case --

THE COURT: All right.

MR. SIEGEL: -- as to Capital One and as to Amazon.

THE COURT: All right. We'll stand in recess.

(Recess from 11:37 a.m. until 11:54 a.m.)

THE COURT: For planning purposes, we'll go until 1:00. We'll break at 1:00 for lunch and resume at 2:00. I want to finish up by 5:30.

How much more do you have on your motion?

MR. SIEGEL: Well, quite a bit, particularly on damages, but it's really a function of if you have questions. I think I can move through it relatively quickly.

THE COURT: All right. Well, I'd like to finish up with your portion by the luncheon break. All right.

MR. SIEGEL: Okay. I will endeavor to do just that, Your Honor.

Thank you.

THE COURT: All right.

MR. SIEGEL: All right. So if I may continue, Your Honor?

THE COURT: Yes.

MR. SIEGEL: Thank you.

So let's move into why we're here, which is class certification. Your Honor, the slides beginning with 73 are the classes that we're seeking to certify here and the representative plaintiffs for each. These are out of our papers, so I won't go through each of them. But each of them identifies the class and the representative plaintiff that is representative of that class, the claims for which the class is bringing those claims, and then the defendants.

So it will say at the end Capital One and AWS, the full class, which is all applicants, that's the 98 million number. We have our representative plaintiffs there. Those claims include breach of contract or, in the alternative, breach of implied contract against Capital One and claims of negligence, unjust enrichment, and declaratory judgment against both Capital One and AWS.

There is an alternative. Again, this is straight out of our papers. I know we don't have all the time in the world, so I won't go through each. But

this tracks our briefing on the identified classes, the alternatives, the California subclass beginning on slide 76.

With respect to the CLRA, that claim is bought only against Capital One and not Amazon because the Court found it did not apply.

As to the Florida claim, that is against Amazon but not Capital One because it cannot be brought against banks.

The New York claim is against both defendants.

The Washington state claim is against both defendants.

So at the conclusion of that portion, you will see in the original presentation I was going to move into standing, but I think we've talked quite a bit about that.

I just do want to touch on slide 84 because I think this is how we finished up. But I just want to emphasize the concept here. We've identified just these examples, but there are more in the complaint. With respect to these three plaintiffs, Zielicke, Gershen, and Sharp, all had fraud. They have sworn in their interrogatories and have been deposed that they have had fraud, and so we think there is little

question that those folks have standing.

And then the only other --

THE COURT: Well, what can the Court consider on the traceability issue? Because, for example, in Gershen's case, his name and his date of birth and some financial information was obtained, likewise with, I think, the other two. Capital One has offered an explanation for why it's not traceable. In your view, can the Court consider that?

MR. SIEGEL: Not for this consideration. It's a contested fact.

THE COURT: What's contested?

MR. SIEGEL: The question of whether the fraud that those representatives have alleged, that they've sworn to, it's evidence. The jury will hear that they've been defrauded in these ways. The jury will hear that the information taken in the breach can be connected to the fraud that they suffered through our experts.

THE COURT: What evidence is that? It's the experts saying, I think that's the case.

MR. SIEGEL: It's the experts saying that this is the nature of data that can lead to a fraud like this. Again --

THE COURT: Well, let's not get into the

other issue.

MR. SIEGEL: Okay.

THE COURT: But you have an explanation for example. I'm not sure exactly which it is but Capital One has offered. For example, he's claiming that he had a credit card opened up in his name which couldn't be opened unless you had a social security number, which wasn't obtained from Capital One. Is that something the Court can consider?

MR. SIEGEL: We don't think the Court should consider that because, again, now we're talking about a factual question. Our expert has said that a social security number or not, this data can be enriched and how it's enriched and why it's valuable to hackers and how they use it. And so we think this is very much a merits question.

This is exactly what this recent *Blackbaud* case decided post *TransUnion*, that this concept of traceability is intertwined with the facts. But based on the same exact claim that -- and, again, back to *Hutton*, *Hutton* says -- again, their defendant was saying, We weren't breached at all. It's not just the data isn't connected or the fraud isn't connected to us. It's we had nothing. We weren't breached.

And the Fourth Circuit said, They claim a

fraud. They claim a fraud that could have been, could have been based on the data compromised in the breach, and that's sufficient for Article III standing.

So if you move beyond that, if you read *Blackbaud*, we think you'll come away with the same conclusion as the court did there, that these traceability challenges, based on whether there is evidence that the breach is connected to the fraud or the fraud is connected to the breach is intertwined with the causation elements of the tort.

THE COURT: Again, what do you think you need to show factually other than having an expert say, "I think it's possible," to establish traceability for the purposes of Article III standing?

MR. SIEGEL: I think we have to allege and have sufficient facts to present to a jury --

THE COURT: Right.

MR. SIEGEL: -- that they suffered a fraud, the type of which could be caused or contributed to cause by the data compromised in the breach.

THE COURT: Why is that sufficiently particularized and not speculative? It could have been. It could have been a lot of things. I mean, doesn't there have to be some concrete traceability to a source?

MR. SIEGEL: I think *Hutton* says no.

THE COURT: Well, *Hutton* is just a -- you pled enough to get past a Rule 12(b)(6) motion.

MR. SIEGEL: But no. It was an Article III question.

THE COURT: Right.

MR. SIEGEL: That's what you're asking. You're asking about an Article III question for purposes of these named representatives.

THE COURT: Right.

MR. SIEGEL: It's the same question. It doesn't change a class certification. There's not a different standard. At trial there might be a different standard, but what you're asking about is a causation question.

THE COURT: No. The standard was did -- was there pled in *Hutton* --

MR. SIEGEL: Say again.

THE COURT: The issue was whether there was pled in *Hutton* facts that made plausible that there was traceability.

MR. SIEGEL: Right.

THE COURT: We're now at the point where you need to present facts that there was, in fact, traceability.

MR. SIEGEL: Right.

THE COURT: All right. And what are those facts?

MR. SIEGEL: But we have presented facts. We have the sworn interrogatory responses that these folks committed fraud. We have a breach with information that our expert could plausibly connect to the fraud, but more than that is a causation question. I think where, respectfully, Your Honor is getting tripped up is there's an element of our claim that's causation, you know, in the negligence claim. I mean, there's not in the breach. The breach is the breach. They were obligated to protect the data, and this is why the breach claim -- they don't challenge standing because once there's a breach, then the law implies harm under Virginia law. So that claim, there's standing, and no one is challenging standing. Capital One is not even challenging standing with respect to unjust enrichment.

They are doing a very narrow argument that goes to causation, and that is what we believe is inextricably tied with the facts that we think the Fourth Circuit has said that is a -- if that is an element of the claim, whether we can establish causation for purposes of our negligence claim, obviously, is a question of fact. You may conclude at

the summary judgment stage. We think not, but a jury will ultimately determine it.

In any event, for purposes of standing, it's not a standing argument. It's a causation argument. It is an element of the claim and one that should not be determined on an Article III basis. We think the law in the Fourth, based on the cases we've cited, is clear on that. And, again, we think the conclusion the *Blackbaud* court reached is right on point as well with respect to that standing question.

THE COURT: All right.

MR. SIEGEL: I know my partner, Lindsay Perkins, can speak for a much longer time on standing, but given the time, I'll move ahead unless you have more additional questions.

THE COURT: All right.

MR. SIEGEL: Let me just turn to the final points on standing. So, again, Capital One doesn't challenge plaintiffs' Article III standing on the unjust enrichment claim, but Amazon does. But, again, like Capital One's challenge -- Capital One is arguing -- I'm sorry. Amazon is arguing that there's a question about whether plaintiffs can demonstrate they conferred a benefit on Amazon.

And this is, again, I think a demonstration

of a merits challenge, and this is explained on slide 90. And, again, as a merits challenge, it is improper for consideration and should be based at trial or on summary judgment and not at the class certification stage. So, again, another merits question.

They being Amazon also make a prudential standing argument. That, too, fails. This is the concept that plaintiffs are attempting to assert a claim that's really Capital One's, but of course, I think the Court made clear in its order on the motion to dismiss in setting out the claims that the way we pled it is appropriate; that is, plaintiffs' claims are premised on Amazon's failure to provide adequate data security to plaintiffs and protect their data. Therefore, the claim for unjust enrichment is appropriate directly, and there's not a prudential standing issue.

Final point: When you look at the *Blackbaud* case, the *Kerns* case from the Fourth Circuit regarding these jurisdictional questions, if they're tied up with causation, they should be treated as merits issues for summary judgment or trial. Again, we think that is very clearly law in the Fourth.

If you go back to *Spokeo* and read what

Justice Thomas says about these common-law claims, they trigger in instances where the state law, where the common law implies a harm. Certainly, that is, we suspect, the reason that Capital One, for example, did not even seek to challenge standing on the breach of contract claim. Those damages, even if they're nominal, are implied.

So let's move on to the Rule 23 standards here. These are well-worn, and I don't think they're in dispute. The first concepts are those of numerosity, commonality, whether the claims are typical of the class, and whether the representative plaintiffs and the lawyers are adequate.

This is a rudimentary pie chart of the size of class against the adult U.S. population. It's a big class. Obviously, numerosity is not an issue. It's like, I think, 12 Virginias. There's about 8.5 million people in this state, Your Honor. It is a large class. Again, the reason I went through that evidence is to demonstrate that the facts underlying plaintiffs' claims apply to these rather large classes all the same way.

At the bench I went through on slide 98 the -- maybe I didn't go through 98 at the bench, David, but I think you've identified this document.

In any event, Your Honor, on page 98 is the numbers that fall into the various classes and subclasses. I think Capital One has asked that that be under seal.

MR. BALSER: (Nods head up and down.)

MR. SIEGEL: I think the common questions are apparent to the Court. Examples abound. We've listed many on page 21 of our brief, including things like did Capital One have a contractual obligation to protect plaintiffs' data, right. There's sort of cross-motions on this issue now. We've, obviously, moved for summary judgment on this very issue. It applies to all 98 million people the same way.

Did they breach? We think that's also apparent from the evidence and can't be disputed.

Likewise, did Capital One and Amazon have a common-law duty to protect plaintiffs' data and, if so, did they breach that duty?

The challenges to commonality are themselves common. And so, for example, the question that Capital One continues to pursue for reasons that we don't quite understand -- but the question of whether noncardholders -- despite Capital One acknowledging the privacy notice applies to applicants, the question of whether noncardholders can assert contract claims under

the privacy notice, they are contesting that. Well, we know who those people are who are applicants, not cardholders, and that's going to rise or fall for all of that cohort of this class. It is a challenge that creates more common issues, not less.

Likewise, the factual question that we discussed at length already, whether there's a risk or whether, in fact, the data was disseminated. We think there's no question that it was disseminated and will be answered the same way from -- we know it was disseminated because they admit that Paige Thompson hacked their systems.

THE COURT: So your view is that there's no need for you to prove anything beyond breach? You don't have to prove any injury beyond breach?

MR. SIEGEL: For standing. For the claim, we do, sure.

THE COURT: So for the claim you need to?

MR. SIEGEL: Yes, and I'm going to get to that.

THE COURT: All right.

MR. SIEGEL: I'm gearing up. I promise.

THE COURT: All right.

MR. SIEGEL: Again, I don't think commonality is seriously in dispute. I would like to just pause on

slide 102. I have about a nine-minute video that I'd like to present. And, Your Honor, look, I mean, there's a lot of lawyers here, dozens. We represent these representative plaintiffs, the putative class here. We have a very short video with respect to the Rule 23(a)(3) adequacy provisions about whether our clients are adequate. We don't believe there's any question about that. If you prefer, I can play it later or just submit it.

THE COURT: If you would, just submit it. This relates to the fourth element, whether they're adequately represented?

MR. SIEGEL: Whether they're adequate and their -- we would like the Court to listen to it.

THE COURT: All right. I'll listen to it.

MR. SIEGEL: They are short clips from their depositions.

THE COURT: All right. Why don't you submit it. I'll listen to it.

MR. SIEGEL: They are Americans from all across the country who have stepped up to serve as representative plaintiffs. It is a diverse group. We have disabled vets from Washington state. We have a retired deputy sheriff from Wisconsin, really a cross-section of, not surprisingly given the class

size, folks all across the country.

THE COURT: All right.

MR. SIEGEL: So let me move to predominance. So in most certification motions, this is where the fight is. It's not Article III standing. It's whether the claims -- the common claims, the common issues predominate. This is perhaps why Capital One is so focused on standing, because there's little question here, despite the class size, that these common issues do predominate.

THE COURT: I mean, the issue is not just whether they're common issues. The question is whether there are common answers to the issues.

MR. SIEGEL: That's right, exactly. We agree. We agree.

Those questions that I posed, does Capital One have an obligation under the --

THE COURT: Right, I understand those. That's why I asked about your view on consequential injury with respect to the breach of contract claim.

MR. SIEGEL: Okay. But here's where that's important. Let me pause there. So I'm going to get to our damages theory quickly -- theories quickly here, but I want to be clear. Our classwide damages theories, how we propose to try this case, we have very

specific classwide damages theories. Those damages theories apply to the class as a whole.

We also recognize, consistent with Supreme Court jurisprudence, like *Tyson*, that there may need to be follow-on proceedings with respect to either unique defenses or unique damages. So, for example, if a plaintiff claims that they have a $1,000 fraud as a result of the breach, we're not proposing that as a classwide damage. That individual -- we would plan to prove up our class representatives, our representative plaintiffs' individual damages with respect to that, but our separate classwide theories of relief apply to the class all the same way.

And I do think that is a critical question you've asked and one I'd like to turn to because I think -- I'm going to move quickly through predominance and then get to the damages.

THE COURT: All right.

MR. SIEGEL: So I think the sort of easiest one to conceptualize under this predominance standard of whether these common issues are more prevalent than noncommon or aggregation defeating issues, in the words of *Tyson*. And again, *Tyson* provides for these -- you can have these separate follow-on proceedings with respect to specific defenses and damages without

impairing predominance.

And so the question at the end of the day, the Fourth Circuit's spin on what the Supreme Court has said about this, is that if common questions represent a significant aspect of the case and can be resolved for all members of a class as a single adjudication, then they predominate over individual questions. And, again, each plaintiffs' claim would not be identical to satisfy that requirement.

So we have the live claims in the case. Count 1 is negligence. Unjust enrichment is 3. Breach of contract is 6. Breach of implied contract is Count 7. I'd like to start with the contract claim. So traditional -- this is slide 108. The traditional elements of a contract claim, you need a legally enforceable obligation. You need a defendant's violation or breach of that obligation. You need injury or damage caused be the breach. Right.

And so, as I said, this question about this promise to protect your personal information from unauthorized access and use and whether they used adequate security measures, Your Honor, both a common question and a common answer, that will be answered the same for all with respect to this promise Capital One made to all 98 million class members.

We can go through chapter and verse on why that's the case and what our proof will be at trial, including our expert, Mr. Kelley, who explains why these standards are required under federal law and why a violation of federal law is violating the obligations under the contract.

So Capital One says a couple of things in response to that. First, they say you can't ascertain the class because there are differences in the privacy notice. There's two privacy notices. We say they say the exact same thing. They say they don't.

Again, if they don't, we know who is in which class. We know who had pre-2010 privacy notices, post-2010 privacy notices. Capital One has that information. And the law is quite clear, as long as you can identify those folks, they do not defeat predominance.

They also raise in sort of a kitchen sink approach this idea that some class members would be subject to a claim that the class member materially breached the contract first. This is an affirmative defense that was not raised, and so we don't think it should be considered at all. In any event, it's clear under *Tyson* that if they have these defenses as to particular plaintiffs, that could be dealt with

posttrial.

Setoff and recoupment, likewise, do not defeat predominance of the contract claim. Setoff is a counterclaim, not a defense, and was not brought. And like first material breach, to the extent the Court would even consider setoff or recoupment, those can be dealt with under *Tyson* in a posttrial proceeding.

Obviously, we have a claim for implied contract that the Court has endorsed to the extent that there is a finding that there's no actual contract, which we think there should be at this point and have moved for summary judgment on that basis.

Similarly, with respect to the unjust enrichment claim, the elements there are the receipt of the benefit and the unjust retention of the benefit at the expense of another.

THE COURT: What slide are you on?

MR. SIEGEL: I'm on slide 117.

We cited in our papers, Your Honor, numerous cases. The *In re Checking Account Overdraft Litigation* cite on slide 118 actually has other cases there. The concept of unjust enrichment claims, given the simplicity of the elements involved, that is, the conferring of the receipt of a benefit and the unjust retention of the benefit, are particularly suitable for

class treatment. And we think here -- if you skip ahead to 119, we -- again, one dataset, all 98 million people. That data was conferred on Capital One. It was conferred on Amazon. Capital One aggregated and mined the data and benefited from its use through its various fraud monitoring programs.

Likewise, AWS, Amazon, used Capital One's data of plaintiffs' PII to generate significant profits. So these are all global questions that can be resolved in one fell swoop for the class.

With respect to the unjust enrichment claim, the finding that this Court made on page 44 in characterizing the claim, we think, you know, again, still applies. This is just a statement of the claim. And whether it is an equitable and unconscionable to prevent the defendants to retain these benefits will be a classwide issue resolved one way or the other, based on the evidence, for all plaintiffs and all class members.

Amazon raises a specific defense or challenge to predominance with respect to unjust enrichment. They have sort of a laundry list, including whether plaintiffs were aware that Amazon was providing any security for the data. We don't think that is an element of the claim and, therefore, should not be

considered.

Likewise -- now on slide 121 -- whether any particular plaintiff had heard of Amazon, not relevant, not an element of the claim. And we've outlined in our papers why the other defenses, we think, are not well taken to predominance of that claim as to Amazon.

There are two cases related to unjust enrichment. One is a Florida case where Florida law specifically requires sort of an examination of each individual circumstances, something that Virginia law does not apply. That would be the *Vega* case, and then defendants also cite this *Grandalski v. Quest* case, a Third Circuit case. But in that case, plaintiffs were refunded overbillings and, therefore, the court found that there was not sufficient predominance in that case, given the individualized nature of these transactions and refunds, to support class certification of an unjust enrichment claim.

Finally, although pled first, our common -- our negligence claim. Obviously, duty, breach, injury are the elements of that claim. We will explain here in a minute why we think we satisfy all of those and what we will present on a classwide basis. Like the contract claim, we think the breach element discussed on page 124 of the presentation is common to the class

and applies classwide. They were aware of the vulnerabilities and risks associated with their systems. They didn't do anything about it, and plaintiffs suffered the harm and resulting damage from that.

The statute of limitations defense, this is a whole separate motion, Judge. This is another item that was raised belatedly. This is part of the Rule 72 appeal, this Capital One notion of adding an additional affirmative defense after the close of discovery on the day we filed our class certification motion. I do not want to get into that. I think that is a separate motion Your Honor is planning to hear tomorrow.

In any event, the timing of when the retention of that benefit became unjust, because of the failure to secure it properly, that's going to be the same for everybody. So, again, we don't think the defense should be in there. If it is in there, the question about timing, there will be a date, and then we will know, based on Capital One's records, who was in and who was out for purposes of recovery for that claim. Therefore, it does not defeat predominance.

There's sort of, again, another kitchen sink effort to suggest that online applications, despite the stated applicability to all applicants, whether, you

know, mitigation can be a defense. These are all issues that, I think, *Tyson* makes quite clear cannot defeat predominance. Therefore, we think this is perhaps, despite the size of the class, the great weight of the predominant common issues really should be not in question, including many of the common issues we talked about with respect to liability. Those will go one way or the other, positive or negative, for the class as a whole. Of course, we're standing here believing they will be positive at the end of the day once heard by a jury.

So, Your Honor, there's a similar analysis with the statutory claims. I would just ask the Court to review our presentation on that. It is consistent with our papers. I was just highlighting the arguments with respect to the statutory claims.

I think the key point there, the damages elements that we will be presenting, the actual damages elements are the same. The statutory claims are not dependent on any misrepresentations. Some cases get tripped up -- I'm on slide 129 now -- around the idea that a state statutory claim or statutory fraud claim is based on a misrepresentation. That is not what the plaintiffs have argued here.

There was certainly a classwide omission, and

that omission is not disclosing that there was inadequate security both at Capital One and Amazon.

Okay. So I've rushed through that so I can bring you to 132, Your Honor, and I think this is kind of where the rubber meets the road. So Your Honor asked about this, as I said, months ago, about what damages are attached to which claim. This chart includes that. So 133 is the Capital One chart, and 134 is the Amazon chart.

And what *Comcast* says, the Supreme Court case, is that as part of the Rule 23 analysis, the Court should consider what damages are applying to what claim. You should avoid sort of the ball of wax approach. So here's what we have. We have this chart and then significant detail behind it, as the basis for each of these damages claims, that will apply to the class as a whole.

So there are -- with respect to Capital One, there are really five categories of damages, the concept of present value of identity theft production is one. The value of access to PII is two. The disgorgement of gains is three. Nominal damages, four, as an alternative to those. And then, of course, if we are successful on a tort, we believe punitive damages are appropriate as well, not listed in your chart but

would apply to at least the negligence claim.

And so the questions that will -- and likewise with respect to Amazon. Obviously, there's no contract on slide 134, so there is no contract claim. And so the claims are limited to unjust enrichment and negligence and, again, we think a punitive basis. The same four categories of damages in addition to the punitives on the negligence claim, the value of the ID protection, the value of access to the PII, disgorgement of gains from the benefit conferred from the PII, and nominal damages apply.

So let me walk the Court, first, through the first theory of damages here, which is the concept of the present value of identify theft protection. So this is the concept, Your Honor, that we were talking about earlier: Will the jury conclude that Capital One's failure to protect this data is such that under the contract claim -- let's just start there -- the jury should award or put the plaintiff class back in the position they would have been but for the breach, that is, their data is protected.

So we have two components of that. One is Mr. Mitnick, who we've talked about, that explains why the class is at current and ongoing risk. And then we have Mr. Long, who is merely presenting an actuarial

exercise of taking the very specific individual class member data about when they were borne and figuring out what it would cost to protect somebody for a lifetime because Capital One failed to fulfill its obligation to do it under the contract. Those numbers are aggregated on page 136.

So, look, we get it. These are big numbers. So -- but I'd like you to look at the top of the chart here where it says average per class member. So if -- Mr. Long explains and provides multiple periods of time. If the jury concludes that class members only need three years of protection, it's $995 per class member. Then if they decide five years, ten years -- and there's a high range, of course, for a lifetime of protection. These are average numbers based on the life expectancy of each class member on the right side.

And so the aggregated classwide damages on the bottom row -- so for all class members to get three years of present value of the monitoring that -- to put them back where they should have been but for the breach, that is a $97 billion price tag.

We recognize, again, it's a big number, but it's very important here to understand, Your Honor, that the big number is a function of the number of victims. And this is a theme we've heard from Capital

One throughout the litigation, certainly in response to the motions before Your Honor today and tomorrow, is that plaintiffs are asking for huge damages.

You know, if there are 50 people in this courtroom, maybe 50 lawyers in this courtroom, and we were here presenting the damages on a classwide basis and instead of 97 million it was 50,000 to provide three years of credit monitoring to put this class, this smaller class in a position plaintiffs should have been in but for the breach, I don't think anybody would be the least bit concerned about that.

And so it is not the $995 or even the $8,369 figure. It's the 98 million people who are in the class, and the reason they're in the class is because Capital One and Amazon breached their obligations to keep this information protected. And this is the way to put them back where they should have been. If they had made like remittitur arguments in response to class certification, which we think should come at the close of trial, not as opposition to class certification.

So the next category of damages is the value of access to class members' PII. Your Honor, in the motion to dismiss phase, rejected the notion that there was a concept of loss of value of PII but this is different. This is the idea -- you will hear a lot

about this tomorrow. Mr. Olsen explains that essentially the plaintiffs here are effectively the equivalent of a patent holder where there is a use of the patent by a noncompeting company, and the relief offered in those cases is a license. And so that is the equivalent of what we have here, and Mr. Olsen calculates that using a standard market approach.

So it is not a diminution in value theory. It's correlated to the value of a license, and I'll explain that in a little more detail here in the final half an hour.

The value of that, again, is quite granular to class members. So this is in his report if you look at Tables 1 and 2 and 9 of Mr. Olsen's report. If you look at the top there, it says range for each class member. That's actually range for each class representative plaintiff. So the range for each representative plaintiff is $14.55 to $30.30.

And what Mr. Olsen did using a lot of data was looked at what the value of this information trades for to come up with a correlated license value for the data that was compromised in the breach. If you look at the range for all class members, it's wider. It's as little as $1.41 per head to as high as close to $300 where all of that data, social security number, bank

account information, was consolidated.

Those tables -- I was going to pop them up on the ELMO, but I think we're running low on time for that -- and walk the Court through it. But those tables show, if the Court looks at table 9, for example, very specifically how those numbers aggregate to the $1,048,130,903 number you see here.

But that's not the result of taking some average or impermissible sampling in the Duke spirit. This is a very specific -- each of those 98 million plaintiffs, we're going to figure out the license value for each of their information. Sometimes it's $1.41; sometimes it's more. If we get a verdict for this claim in this amount, we can distribute that money to those plaintiffs in the amount identified in Mr. Olsen's report.

Finally, we have the disgorgement of gains from the benefit from using the PII. We've already talked about this a little bit in terms of the unjust enrichment claim, but Mr. Olsen calculates both the benefit to Capital One and the benefit to Amazon as a result of using plaintiffs' PII without protecting it.

Your Honor, Mr. Newby told me he believes the next page, 140, is under seal. So I'll just reference it here. Those are the totals -- oh, I'm sorry. Those

are the totals reflected for both Capital One and Amazon.

The Capital One numbers, you will see, are divided between those former and current customers that entered into a cardholder agreement and those that were not. Remember, Capital One used all of that data whether or not they were cardholders ultimately.

On the Amazon side, you will see the calculation that Mr. Olsen undertook with respect to the revenue and then the profit margins enjoyed by AWS as a benefit from using and housing plaintiffs' PII while not maintaining adequate data security.

So what is the test here? On page 141, I mentioned the *Comcast* case. The important thing is that the models measure damages to each class member resulting from the defendants' conduct, and that's exactly what we've done here. And we believe we've met the standard perfectly. We've spent a lot of time on it. We think it meets the standard set forth by *Comcast*. Our damages theories are attached to our claims, and we're prepared to present these at trial. It's all math at the end of the day.

Now, how are those claims tethered to these damages theories? So I started to talk about slide 142, which is this present value of the identity

protection services as contract damages. So Virginia law applies to restatement of contracts. And, again, it's the concept found in Section 344 of the restatement, which has been cited numerous times by Virginia courts, that the goal of remedy for a breach of contract case is to put the class in as good a position as they would have been in had the contract been performed, that is, had there been no breach.

Obviously, plaintiffs here are in the class. The expectation, the contractual expectation was that Capital One would protect their PII and not increase their risk, which I don't think is in dispute here as to whether the risk is increased. In any event, it's a triable issue.

And then, of course, how to restore that contractual expectation. We believe the appropriate way to do it is provide the protection that Capital One promised and then failed on, which is protecting this information going forward through this monitoring product for which we've taken to a present value for damages purposes.

Your Honor, starting at slide 143, we do a deeper dive into the restatement. As I said, we've spent substantial time, and I would like to go through this with you.

THE COURT: Well, this is what we're going to talk about tomorrow; isn't it?

MR. SIEGEL: I'm sorry?

THE COURT: This is what we're going to talk about tomorrow?

MR. SIEGEL: I don't know how much this is going to come up tomorrow. So let me just walk through it. I think I can get through most of it in about 20 minutes here.

THE COURT: All right.

MR. SIEGEL: I just -- what I want to do, at least for purposes of this argument and how it relates to class certification and these damages theories being grounded in solid Virginia law tethered to our claims on behalf of the whole class, for purposes of certifying the class, that's really the goal for today.

So we add a little more detail here on 143 about there's two ways to conceptualize this, the value to the plaintiffs or the cost of remedy, the breach of Capital One's failed performance. These, again, are concepts under the restatement, Sections 347 and 348(2)(b). We believe that a court -- I'm sorry -- a jury can easily find that those are appropriate mechanisms to determine that this relief is appropriate.

So under that first one, under 347, the concept of this present value of credit monitoring, as a measure of the value of Capital One's contractual performance, that is one way to think about it. Buyers, you know, willingly purchase products and services that safeguard PII. I mean, those are open-market products, so we're able to value those. We think that is exactly what the restatement says about using that value as a fiat for Capital One's performance of its promise to protect the data.

The next concept is just a little different under 348. That is the -- the concept of this credit monitoring is a measure of the cost to remedy Capital One's defective performance. You can either -- you can do two things with this data. You cannot disclose it, which is what Capital One promised or -- now once disclosed, now that the cat is out of the bag -- and Mr. Mitnick is quite clear about this part, that the only way to protect it at this point is to actively monitor. So because it can't be undisclosed under 348(2)(b), we think this is a second basis to support a contract theory applying the concept of present value of future monitoring.

We also think, as we -- on those initial boxes, you will see a checkmark for these damages as it

relates to negligence as to both Amazon and Capital One. We walk through in these slides, Your Honor, the concept of medical monitoring. The defendants have argued that medical monitoring concepts are inapplicable because there's no present injury. We believe that is not the case here because we can show that, unlike medical monitoring cases that the defendants have raised, here we have the value of identity theft protection is accompanied -- it's not sitting out there naked. It's accompanied by a presently compensable injury in the form of this value of access to plaintiffs' PII, the concept of this royalty that I'll talk about here shortly and, therefore, we think is well supported by established Virginia common law.

So to do a little bit of a deeper dive as it relates to using this value identity protection services as a theory of damages for the negligence claim as to both defendants -- so this perhaps gets to an earlier question on standing, but I just -- the concept held in restatement of torts, again, frequently cited in Virginia law, this specific section, 910, says, One injured by the tort of another is entitled to recover damages from the other for all harm, past, present, and prospective, legally caused by the tort.

And so the concept of this credit monitoring cost to repair the confidentiality of the PII are these future mitigation costs referred to in the restatement, and these include expenditures reasonably made in an effort to avert the harm threatened by the defendants' conduct. And we think that applies to both Capital One and Amazon.

Alternatively, under Section 928, you will see there's a basis under Virginia law for cost to repair. When diminution in value is not available, as it's not here, the alternative under Virginia law is to measure damages as the reasonable cost of repair under a negligence theory.

So that's, in a nutshell, the value of identity protection services, the present value of that and how that is captured by our claims.

Let me turn to the value of access to PII. This begins on slide 149. This is Mr. Olsen's report. He walks through in great detail the concept of this, of the nonpracticing patent owner who's been damaged through the unauthorized use of the patent. So this is a concept where, in this instance, when you have this type of patent infringement by a noncompetitor, the damages are a reasonable royalty. We think that can correlate precisely, precisely to the facts we have

here.

The threshold for that, beginning on 150, is accepting, Judge, the threshold question of whether there is a protectable property interest in personal information. I think -- I don't think there's anything in your order that sort of decided that issue one way or the other even though it was discussed at the motion to dismiss phase.

But the concept of a protectable property interest is certainly well supported in data breach cases, *Marriott* being one of the most recent that Your Honor cited for a different proposition in the order on the motion to dismiss. In that case, Judge Grimm collects the cases for the, quote, growing trend across courts that have considered the issue to conclude that individuals have property interest in their personal information.

And so that is a threshold question. Obviously, it applies to the class as a whole. Either it is or it isn't. We think the Court will ultimately conclude that is a protectable property interest.

So the concept of a reasonable rental value for damages associated with unauthorized use of personal property, which is what we have here, that is contained under a statement of torts at 931, at

Comment A. And that rental value is the market value. They have similar transactions. That's exactly the exercise that Mr. Olsen took here.

This can also be applied to a contract theory as to Capital One, the concept of value of an unauthorized access as a measure of restitutionary recovery for a breach of contract. This is Section 42 of the restatement of restitution that recognizes these patent-like damages, measures for unauthorized use beyond the traditional IP categories. They are comparable to rights that control the use of any idea, expression, or information. Again, really consistent with what Justice Thomas has said throughout his jurisprudence about these common-law claims and personal privacy rights and interest in your own information. We identify the specific comments to the restatement that provide for these restitutionary type values as relief for a breach of contract claim.

Finally, disgorgement. Obviously, it's tethered, in the first instance, to unjust enrichment. The concept of disgorgement is measured by the benefit realized and retained by the defendant. That is the Virginia Supreme Court. And that benefit is quite broad. The restatement provides it can be profits, but it can also be things like savings and other

consequential gains from retention, in this case, of plaintiffs' PII unjustly.

So with respect to Capital One, on slide 153, we -- they were certainly enriched by the use of class members' PII as a nonreturnable benefit. We have specific dollar values associated with that benefit that are in the summary chart under seal I referred to earlier. And it can be measured by the value of -- that harm, that damage can be measured by the value of the benefit in advancing the purposes of the defendant, and that's what Mr. Olsen has done here.

And the fraud loss is avoided through modeling using class members' PII, including people who were never cardholders. They were just applicants. They're using all this data. We believe that is an appropriate theory of damages for unjust enrichment.

THE COURT: One question I had about the unjust enrichment. As I understand the theory, it's that somebody provided a benefit for which they have not been compensated. Correct?

MR. SIEGEL: No. It's provided a benefit, the retention of which, under the circumstances, is unjust.

THE COURT: Right.

MR. SIEGEL: So that's a little different

than looking at the benefit conferred to the plaintiff. It is a -- it's, obviously, a broad spectrum of factual scenarios that may fall under that. But if the plaintiffs conferred their personal information and the defendants retained that under circumstances for long-term --

THE COURT: That are unjust.

MR. SIEGEL: That are unjust.

THE COURT: In assessing the circumstances, though, you need to consider what the person providing the information received in return.

MR. SIEGEL: I can --

THE COURT: How would you otherwise measure unjustness?

MR. SIEGEL: Yeah. Well, I think that is a circumstance, sure. I think that may be in the panoply of circumstances a jury can consider on whether it's just or unjust. Sure. And I think, obviously, we think the facts here are going to suggest that that retention is unjust.

Disgorgement, it can also be an alternative to the contract remedy. So where a breach is deliberate -- this is citing a Pennsylvania case, but this refers to the restatement. If there is a deliberate breach of a contract that results in profit

to a defaulting promisor -- in this case, Capital One -- the available remedy -- again, only Capital One has the contract. So the available remedy -- this would only apply to Capital One -- affords inadequate protection to the promisees' contractual entitlement.

So if for some reason there is not a finding of damages with respect to the contract claim, the jury can consider this disgorgement theory as an alternative. And I do believe it would be an alternative under this particular theory of damages under the contract claim.

We provide there the concept of cost savings under the restatement, which is what certainly we have in the case of Capital One in support for our unjust enrichment claim, and how they used plaintiffs' PII for fraud modeling conferring this benefit that was retained unjustly.

With respect to this claim against Amazon, the unjust enrichment claim, the Court touched on this. This is slide 156. Plaintiffs, obviously, directly transacted business with Capital One, but I think the Court understood the claim here that ultimately there was a benefit conferred on Amazon by Amazon's use of that PII. And, again, Amazon profited, and we have Mr. Olsen providing the profit calculations based on

Amazon's retained benefits from retaining plaintiffs' PII and, obviously, a function of its contracts with Capital One.

Finally, Your Honor, nominal damages. So the case I was searching for earlier is *Paulette*, among others. *Kerns v. Wells Fargo* is probably the key one, 818 S.E. 2d 779, which is a Virginia Supreme Court case. This is the concept that once there is breach, the law infers damage.

And so this touches on the standing question, but clearly, if there is a legal threshold to damage, there's Article III standing. But I don't want to rehash that argument.

THE COURT: All right.

MR. SIEGEL: It is the case I was searching for earlier that I could not come up with when we were talking about this. So here it is. It's *Kerns*.

The concept here is nominal damages as to the breach of contract claim initially. This is the minimum recovery if the jury does not accept our other theories of damage but finds breach. In other words, if they find breach -- if they find we've met the elements but did not -- if they find we've lacked proof in quantifying the damage, we're entitled to nominal damage.

THE COURT: Well, I mean, nominal damages -- and I understand these cases are a little unclear about exactly what they're talking about. But as I read them, I understand nominal damages to essentially be a default measure of damages in a breach of contract case for a proven injury. It doesn't mean you get nominal damages where there's no injury. It's where you have injury that can't be measured or people chose not to measure. It's the default measure of an injury.

MR. SIEGEL: Of damage.

THE COURT: Of damage, yes.

MR. SIEGEL: Yes, agreed.

THE COURT: Flowing from an injury.

MR. SIEGEL: Correct.

THE COURT: All right.

MR. SIEGEL: So the concept of nominal damages, again, in this *Kerns* case where there's a legal right to be vindicated where there has been no actual present or loss of any kind where from the nature of the case some injury has been done but the proof fails to show the amount, which I think is exactly what Your Honor just said --

THE COURT: Right.

MR. SIEGEL: -- that's *Kerns*.

And so, again, we think, you know, this is a

jury question: Is there an injury? And the jury may find, yes, injury, but reject our damages theories. We hope not. But if that's the case, we would be entitled to nominal damages at that point as an alternative remedy.

And so just the concepts here. Because this has come up in various arguments on unrelated issues and certainly has been injected as part of the certification question. The concept of nominal damages in a class action cannot be diminished because there's 98 million people. That would be a plain violation of the Rules Enabling Act, which can't increase or decrease the rights of individuals, and Rule 23 wouldn't permit Capital One to attempt to subvert that right, individual right, through Rule 23.

So each individual would be entitled to -- if we prove the elements of our contract claim but not this damage to specificity -- a nominal damages for breach of contract -- there are cases all over the map. It's our view -- and we'll ask for $100 per class member. Again, I think Capital One has objected to that as being somehow outrageous.

Again, Your Honor, I would just put it to the Court this way: $100 per head of people in this room, you know, we're talking about $5,000. The function of

the large numbers, if it's $100 a head and we're at $9.8 billion, that is a function of Capital One's failure to protect this data for this massive group of people. That's not the plaintiffs' fault.

And so individually, even for a nominal damage, $100, which has been accepted by Virginia courts, we would think would be appropriate as an alternative remedy, again, not something that needs to be determined as part of the class certification but something that is surely going to be briefed down the pike.

So there are -- there is a basis for nominal damages as well for unjust enrichment. We've cited cases on slide 159 where, again, if we meet the elements, damages are unproved, then we are in the nominal damages territory with respect to the unjust enrichment claim.

Slide 160 provides a similar basis to consider nominal damages with respect to the negligence claim. Again, I would just ask the Court to look at the *Kerns* case, *Kerns v. Wells Fargo*, the Virginia Supreme Court case, which talks about the concept of nominal damages to vindicate a right where there's -- in negligence where no actual loss occurred. Here, again, we think there has been an actual loss that has

occurred, and that's the concept of this royalty value, this rental value that Mr. Olsen has put on behalf of the plaintiff class that makes that injury or damage current and, therefore, appropriate for a negligence theory.

I will -- because actual damages are available, all of these damages theories I've just described are available under the state statutory claims -- I won't go through them -- and that begins on 161 for detail.

The actual damages are available under New York, Washington, California, and CLRA. All the theories, the theories of loss market value of access to PII, the actuarial present value of the identity theft protection are -- the rental value, I should say, and the actuarial present value of identity theft protection are actual damages available under these state statutory claims and satisfy as well restitutionary claims under California's UCL and CLRA.

Finally, the next slide is the same with respect to Amazon. It includes a Florida statute which was not included in the prior slide. It excludes the CLRA which was included as to Capital One but otherwise identical with respect to what damages are available under those state statutory claims.

So I think I've addressed the predominance issues, as I've gone through here, that defendants have raised.

And in my final two minutes, as I'm going to dutifully stay to the Court's limitation here, is the concept of superiority. So this is under Rule 23(b)(3). This is a critically important idea, and that is that a class action is the right tool to resolve these issues.

So I think the -- and there's elements under Rule 23(b)(3) which should be considered by the Court. But the concept that a class action is superior to having 98 million people come through your doors or even a tiny percentage of that, we think it's unquestionably the right way to resolve these issues for good or ill as to the plaintiff class. Maybe the defendants will win, but they'll win as to the entire class. And we just think that is the appropriate way to deal with a case that has this many common issues that will transfer across all 98 million class members.

It is also quite clear that under 23(b)(3)(A) that the realistic alternative to a class action is no recovery for these plaintiffs, and we think that is an important consideration. You can see what is lined up to my right back here. They have an incredible legal

team that is fighting this case tooth and nail, and for an individual to do battle against Capital One and their lawyers, it really means there is no alternative to a class action. That is a consideration under Rule 23(b)(3)(A) and one that the *TD Bank* case we cite on slide 171 talks about.

We also satisfy (3)(b) and (3)(c) as superiority concerns. I think if you look at *TD Bank*, that goes actually through superiority. It's very similar. You have a common contract, a form contract, and the issues in *TD Bank* are very similar -- in the certified case, very similar to the issues present here.

Finally, certification under 23(b)(2), this is Count 4 for declaratory relief. That is appropriate under (b)(2) when a party opposing the class has acted or refused to act on grounds that apply generally to the class making final injunctive relief appropriate.

The relief here is definite and concrete we are seeking, the injunction we're seeking regarding the protection of this data as to both Capital One and Amazon. The injunction is not seeking damages. So there's no question that we're not trying to jam a damages theory into a (b)(2) certification, which sometimes has gotten plaintiffs into trouble. But it

is purely a separate injunctive relief with respect to ensuring the protection of this data on a prospective basis.

And our expert describes in great detail what is necessary to satisfy a reasonable security standard, included -- summarized in slide 178 where Professor Madnick explains what is necessary to ensure that this data is protected.

Finally, issue certification. Really finally, I think. We're close to really finally.

Issue certification, we don't -- you know, Rule 23(c)(4) is something we moved under. We think it's appropriate to certify --

THE COURT: I've seen that.

All right. We're going to go ahead and break for lunch.

MR. SIEGEL: Thank you, Your Honor.

THE COURT: We will start at 2:00 with Mr. Balser.

MR. BALSER: Thank you, Your Honor.

THE COURT: The Court will stand in recess.

(Recess from 1:03 p.m. until 2:03 p.m.)

THE COURT: Mr. Balser.

MR. BALSER: Thank you, Your Honor. David Balser on behalf of Capital One.

I would like to take the Court up on its invitation to begin argument with a focus on standing, and I agree with the Court that the issue with standing is imminently bound up with the class certification issue. So I do think it makes sense to spend some time working our way through the standing issues.

And like Mr. Siegel, we have prepared a PowerPoint that we think will assist or hope will assist the Court as we go through the argument.

THE COURT: All right.

(Documents are passed up to the Court.)

MR. BALSER: And I'd like to do a deep dive into standing before we turn to the Rule 23 predominance arguments and the other Rule 23 arguments that we have.

To begin, the eight representative plaintiffs -- and that's really all the Court can focus on here. There's 98 million absent class members, but there's 8 representative plaintiffs whose claims are at issue here. Not one of them has suffered an injury that's sufficient to confer standing for this Court to hear their negligence, statutory and injunctive relief claims under Article III.

Plaintiffs' standing is foreclosed by two Fourth Circuit cases, which this Court is now very

familiar with. The *Beck* and *Hutton* cases, as well as the Supreme Court's recent decision in *TransUnion v. Ramirez*. The Court must resolve this challenge to its jurisdiction to hear those claims before addressing any of the other pending motions, including plaintiffs' motion for class certification, because plaintiffs who lack standing cannot pursue claims on behalf of an alleged class. That's just black-letter law, and plaintiffs' invitation to delay the consideration of the standing issues is inviting error.

Fortunately, deciding this jurisdictional question at this stage of the proceedings is a straightforward matter because the record evidence is now established, and it clearly shows that these eight representative plaintiffs have not been injured by the cyber incident.

THE COURT: How does the Court do that? Under a summary judgment standard?

MR. BALSER: It is a summary judgment standard, Your Honor, absolutely. Could a reasonable juror conclude, based on the evidence, that the plaintiff has shown that it has suffered an injury-in-fact that is traceable to the data breach? That's the standard.

THE COURT: Okay.

MR. BALSER: And it's not a jury question. It's a question for the Court to decide. The jury doesn't get to decide Article III issues. It's the Court --

THE COURT: Well, under the summary judgment standard, the issue is whether there's a factual issue or whether there's no genuine issues of disputed fact.

MR. BALSER: No genuine issue of disputed fact from which a jury can conclude the standing.

THE COURT: Right.

MR. BALSER: And I think we all agree on what the summary judgment standard is, and we agree that that is the standard that the Court should apply.

THE COURT: Right. But those facts under the summary judgment standard are to be viewed most favorably to the plaintiff with all reasonable inferences drawn in their favor. So if the Court were to conclude, based on that standard, that there's a genuine factual issue, then that would go to the jury?

MR. BALSER: Well, the Court would then have established that the plaintiffs have standing. We still would have our arguments under Rule 23, and we have a summary judgment motion that's pending. So we would say, no, it's never going to get to the jury, you know, once the Court takes up our summary judgment

issue, but it would have passed the --

THE COURT: All right. I understand, the standing issue.

MR. BALSER: It would have passed the standing threshold.

THE COURT: All right.

MR. BALSER: So let's be clear what claims we're asking the Court to dismiss under Article III. It's three sets of claims, the negligence claim, the state statutory violations, and the injunctive relief claim.

As Your Honor well knows, Article III requires plaintiffs to invoke the jurisdiction of a federal court to establish standing. Much of the argument that I heard this morning from Mr. Siegel attempts to shift the burden to the defendants to prove that the plaintiffs don't have standing, but that's not the standard. It's the plaintiffs who have the burden to show standing, and to establish standing, they have to show that they suffered an injury-in-fact that's fairly traceable to the challenged conduct of the defendant and it's likely to be redressed by favorable judicial decision. We don't contest redressability here.

Because discovery has closed, plaintiffs must

prove their standing with evidence. The Fourth Circuit's cases are clear about this fundamental requirement, which descends from the Supreme Court's decision in *Lujan*. In *Beck*, the Fourth Circuit held that because the plaintiffs had developed a summary judgment record, they were required to prove their standing with evidence and specific facts.

We cited the *Libertarian Party of Virginia v. Judd* case, which is another Fourth Circuit case that held that following the close of discovery, plaintiffs were required to establish their standing with evidence. And as Your Honor properly noted, the proper evidentiary standard resembles summary judgment.

In the *Department of Commerce v. U.S. House of Representatives* case, the Supreme Court held that to proceed to trial, plaintiffs must establish at least a genuine issue of material fact as to each element of their standing. And as I said before, importantly, this is a threshold consideration that the Court needs to take up. This means that plaintiffs here are required to make this evidentiary showing at this juncture before this Court considers whether to certify a class.

Under the Supreme Court's decision in *Steel Company v. Citizens for a Better Environment*, it's not

appropriate for district courts to exercise hypothetical jurisdiction over actions where as a matter of fact standing has not been established. Indeed, in the *Rivera v. Wyeth*, this Fifth Circuit case that we've cited in our motion for leave to file supplemental brief on *Ramirez*, the Fifth Circuit held that it was reversible error to certify a class where the named plaintiffs clearly lack standing. We cited both of those cases, both *Rivera* and the *Steel Company* case in our papers.

As I'm going to discuss in a little more detail here in a minute, no class should be certified in this case in any event, but the Court shouldn't even reach that issue and inquiry until it assures itself that it has jurisdiction over the claims of the named plaintiffs.

So how does the Court make that determination? Fortunately, the Fourth Circuit has provided ample guidance on this. It is twice considered in the context of claimed data breaches whether plaintiffs have standing. *Beck* and *Hutton* both make clear that the mere compromise or theft of data fails to satisfy the injury-in-fact requirement of Article III. I'll get into the facts of those cases in a little more detail in a minute, but the upshot of

Beck and *Hutton* is that plaintiffs cannot establish standing based on the mere fact of a data breach.

As the Court well knows and we briefed, the Supreme Court recently considered standing in the *TransUnion* v. *Ramirez* case. There the court affirmed the fundamental requirement that plaintiffs must prove a concrete injury-in-fact to invoke the jurisdiction of a federal court. Justice Kavanaugh writing for the court said not once but twice, no concrete harm, no standing.

The Supreme Court held in that case that plaintiffs do not have Article III standing to seek damages based only on a future risk of harm. That is clear from *Ramirez*. The court recognized as persuasive *TransUnion*'s argument that in a damages suit -- and I quote -- The mere risk of future harm, standing alone, cannot qualify as a concrete harm.

The court adopted that reasoning as the basis for its decision when it said, Here the 6,332 plaintiffs did not demonstrate that the risk of future harm materialized. Therefore, their damages claims, based on an unasserted risk of future harm, is unavailing.

Thus, the real risk of harm under *Ramirez* -- the risk of real harm must either materialize into an

actual harm or cause some independent harm to occur in order to confer standing.

THE COURT: The Court in *Hutton* distinguished *Beck* on the grounds that in *Beck* all there was was the theft of a computer that happened to have personal information on it and distinguished *Beck* from the allegations in *Hutton* that there was a targeted hack for the purposes of obtaining personal information. The court, I believe, said for the purposes of establishing plausibility, you could reasonably infer that somebody who targeted personal identification did so with the intent to use it in some fashion. It was really on the basis of that, I think, that they said you can infer plausibly actual harm for the purposes of Article III standing.

What's unclear to me is whether the reasonable inference is still reasonable in light of what *Ramirez* has to say.

MR. BALSER: It may not be, and I think it's a really good question. I think that, you know, there are a couple of differences between *Hutton* and *Ramirez*. *Hutton* was decided on pleadings. It was a facial challenge, not a factual challenge. And *Ramirez* certainly occurred after a full evidentiary hearing.

But I do think, you know, in *Ramirez*, even

if -- like, to take the facts of our case, I mean, even if the plaintiffs could prove there is dissemination of the data, which they haven't, I don't think that gets them far enough under *Ramirez*. Whereas under *Hutton*, it might have. So I think there may be some curtailing of the rationale in *Hutton* by *Ramirez*. I think *Hutton* actually helps our case, even though the Court found standing there, because I think it shows what a plaintiff would have to show to satisfy traceability. The facts of that case were really pretty compelling at least as alleged.

In that case, there were members of an optometry association who over a course of years had provided PII, including name, date of birth, social security number, in order to take the optometry exam to get licensed. And what started happening is a number of these people, all of whom were members of this association who had provided that information, all started getting false Visa cards opened in their own names. Some of those names were maiden names that had been provided only to the optometry association 20 years ago.

And so when you look at the facts as alleged there, the court, I think, correctly found that traceability had been met. That's a far cry from the

circumstances that we have here, and I'm going to go through the individual plaintiffs in a little bit of detail here to show the differences.

But I do agree with Your Honor that I think *Ramirez* is a game changer, and I do think that fairly read, the rationale in *Hutton* may no longer hold up under *Ramirez* where future risk of harm is just clearly insufficient to support standing.

THE COURT: Well, that's the issue. Can you establish Article III standing in the absence of materialized harm based on the threat no matter how substantial?

MR. BALSER: I think the answer is clearly no after *Ramirez*. I just think the answer is no. And I think there's other *indicia* in *Ramirez* that supports that conclusion. For example, the court in *Ramirez* made clear that courts are not permitted to redress legal violations absent concrete harm. There was that great quote that Justice Kavanaugh used from the *Casillas* case that Justice Barrett had written when she was on the Seventh Circuit which said that Article III grants federal courts the power to redress harms that defendants cause plaintiffs, not a freewheeling power to hold defendants accountable for legal infractions.

Without proof of an injury-in-fact, this

Court cannot award plaintiffs damages here by holding Capital One accountable for some legal infraction that caused no harm. I mean, I think they're absolutely clear. You have got -- it has to be a concrete particularized materialized harm in order to meet the standard for Article III.

So I think the key takeaways under *Ramirez* are a plaintiff has to have suffered concrete harm to have standing to seek damages. The mere risk of harm is not concrete under *Ramirez*, and federal courts don't have some freewheeling power to correct a violation of law divorced from actual injuries. That's what the court says.

So before I get further into the core Article III arguments and apply them to the facts here, I do want to address the plaintiffs' arguments on *Ramirez*, some of which Mr. Siegel made this morning, some of which were in the briefs.

THE COURT: All right.

MR. BALSER: In a recently filed supplement brief and some this morning, the plaintiffs have tried the gloss over *Ramirez* with three incorrect arguments that are unsupported by that opinion. This is what they rely on to try to get by *Ramirez*.

First, they argue that they have standing --

this is their argument -- that they have standing to assert their negligence claim because it arises under common law. That's their argument. The second one is they have standing because they seek damages. And their third argument -- and I want to spend some time on this because Mr. Siegel spent quite a bit of time on it -- they say that this Court should assume standing because the issue is intertwined with the merits. Each of these arguments is wrong, and I want to just briefly address each of them in turn.

So let's start with this theory about common-law right. First, the plaintiffs incorrectly argue that they've established standing by merely alleging the violation of a common-law right as opposed to a statutory right. Asserting a common-law right does not automatically grant standing. *Ramirez* did not hold that, and no other Supreme Court case has either.

In fact, *Ramirez* states an injury-in-law is not an injury-in-fact, and they go on to say that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm. *Ramirez* simply does not limit the concrete harm requirement to statutory violations. Plaintiffs' negligence claim here alleges only an injury-in-law. That is not sufficient for standing.

Now, plaintiffs have not cited a single case, not one, applying this theory of standing, which would mean that plaintiffs would always have standing to assert any tort claim. *Hutton* forecloses that theory. There the Fourth Circuit held that plaintiffs had standing to sue for negligence but only after painstakingly analyzing whether they had, in fact, alleged an injury-in-fact.

In fact, if we put up on the slide here the entire opinion in *Hutton*, two pages of that opinion were devoted to analyzing whether there was an injury-in-fact sufficient to support standing. In plaintiffs' view of standing, that was an unnecessary analysis.

And as we talked about a minute ago, the plaintiffs in *Hutton* had standing or were found to have standing because they had alleged actual fraud and had tied that fraud to the only common source of the plaintiffs' data; that is, they alleged that the injury was traceable to the defendant.

I think it's just worth noting that this argument would apply only to the negligence claims in any event and not to the state statutory claims, which, of course, are not common-law rights.

I think it's also important to note on this

theory of, you know, because we've alleged negligence, we get into federal court, courts in data breach cases, both within the Fourth Circuit and outside, routinely dismiss negligence claims for lack of standing. On this slide here that we have, we've listed ten cases, all of which are data breach cases, that were dismissed by courts for failure to plead or prove standing in data breach cases. At least two of those cases were affirmed on appeal by the Eighth Circuit and the Third Circuit.

In contrast, plaintiffs have not cited a single case adopting their novel theory of standing under which a plaintiff can always assert any common-law claim in federal court even if they were uninjured. They rely on a couple of cases, each of which is in apposite. The one I like the most is the *Whittemore v. Cutter* case. That's a 208-year-old patent case.

Even if that case suggests that legal violations are injuries -- and I invite the Court to read that opinion and see whether the Court can find that inference anywhere in there -- *Ramirez* says the opposite. *Ramirez* is clear that an injury-in-law is not an injury-in-fact.

They rely on the *FMC Corp. v. Boesky* case,

which is a Seventh Circuit case. That was a case that dealt with common-law actions that do not require a proof of injury, like fiduciary duty claims, and they say so in that decision. That case does not hold that plaintiffs can seek compensatory damages under a negligence theory without proving that they've been harmed.

Plaintiffs also rely on Justice Thomas' concurrence in *Spokeo*. Of course, a concurrence is not the law. The *Spokeo* majority held that to establish an injury-in-fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized. That's two separate inquiries. The law asked whether there's been a legal invasion, and the second question is whether that invasion is concrete. The upshot is that legal invasions are not always concrete.

They cite the *Servicios* case, which is a breach of contract case, and it does not hold that negligence claims can proceed without proof of injury. They cite the Supreme Court's decision in the *Uzuegbunam* case.

Easy for me to say. Good luck with spelling that one, Ms. Montgomery.

That case involved a constitutional violation

which is clearly an injury-in-fact. The court's opinion in that case was limited to nominal damages and redressability. It says nothing about whether uninjured plaintiffs have standing to claim compensatory damages for negligence.

They mention in a footnote in their *Ramirez* brief that they would still have standing notwithstanding *Ramirez* because the harm they allege is similar to disclosure of private information, which the Supreme Court recognized in *Ramirez* as a common-law harm. There's a reason that one is in the footnote, not in the text of their brief. Capital One did not disclose plaintiffs' information here. The information was stolen from Capital One, and much of the information at issue here was already public anyway, as the Court knows. There is no common-law liability and analogous circumstances, and *Ramirez* does not suggest otherwise.

This theory is also foreclosed by *Beck* and *Hutton*. *Ramirez* does not overrule or abrogate those cases except, I think, as Your Honor pointed, that some of the reasoning in *Hutton* about traceability might not still be good law after *Ramirez*. I think *Ramirez* does go farther than *Hutton* did, but those cases clearly hold that mere exposure of data does not create

standing. Certainly, those holdings have only been reinforced by *Ramirez*, not stirred by it.

The next argument is a really interesting one. They argue that because they allege damages, they automatically get into federal court. But a claim for money damages does not mean that plaintiffs have suffered a monetary injury. Plaintiffs cite no case adopting that extreme position. Although *Ramirez* did recognize that monetary injuries are classic harms in common law, it does not follow that a mere allegation of money damages is enough to establish standing.

Plaintiffs' argument conflates damages, which is an element of their negligence claim, with injury, which is what Article III requires. The fact that a plaintiff seeks money damages for a noninjury does not morph the noninjury into an injury-in-fact, and *Ramirez* suggests as much when the court said the mere risk of future harm, without more, cannot qualify as a concrete harm in a suit for damages. The allegation of damages itself is not a concrete harm. Otherwise, plaintiffs could get into federal court with only frivolous damages allegations, and that's not the law.

They argue quickly and briefly about mitigation expenses. They argue that the claim for mitigation expenses saves the risk of harm theory, but

mitigation expenses are not analogous to the separate concrete harms identified by the Supreme Court in *Ramirez*. They simply don't have a common-law cause of action based only on mitigation expenses, let alone mitigation expenses that are incurred in response to a nonimminent risk, which have clearly been foreclosed by both *Clapper* and *Beck*.

Here is the argument I want to spend the most time on that they made, which is this argument about the standing issue being intertwined with the merits. Basically, what plaintiffs are asking the Court to do is kick the can down the road on standing because these issues are intertwined. But if plaintiffs cannot show a genuine issue of material fact as to their standing -- and they cannot -- then dismissal for lack of jurisdiction is required and plaintiffs cannot proceed to trial on those claims. That's the teaching of the Supreme Court's *Department of Commerce* case.

Plaintiffs' argument that this Court can assume jurisdiction is not the law in a case that is proceeded through discovery where plaintiffs must prove their standing with evidence. In addition to *Beck* and *Libertarian Party of Virginia*, which we discussed a few minutes ago, the Fourth Circuit in this *Baehr v. Creig Northrop Team* case quoted the Supreme Court's decision

in *Lujan* for the proposition that plaintiffs -- and I quote -- are obliged to set forth by affidavit or other evidence specific facts that when taken as true establish each element of Article III standing.

This next slide, Your Honor, I think is the most important one. Tellingly, the only cases that plaintiff cite are cases that were decided at the pleading stage, which we are far past. You asked Mr. Siegel, and I wrote it down: Can I consider these issues, these fact issues now?

And Mr. Siegel said: No, you can't because -- and he cited you to the *Blackbaud* case. The *Blackbaud* case is dispositive, he said.

That's a Rule 12(b)(1) case that was decided on the pleadings. There's not one case that they cite that is not a facial challenge at the 12(b)(1) stage. The time to decide whether the Court has jurisdiction is now, not sometime in the future.

Plaintiffs have had two years of discovery to come up with evidence that they've been harmed, and they haven't been able to do it. Discovery is closed. Cross-motions for summary judgment are on file, and the law is clear that plaintiffs have to prove their standing with evidence. Plaintiffs argument to the contrary is just incorrect.

Having taken the *Ramirez* issues off the table, I want to just quickly address the core Article III arguments. And the Court is familiar with *Beck* and *Hutton*. I'm not going to belabor the cases, but you know, the Fourth Circuit in *Beck* clearly held that the mere theft of plaintiffs' data, without more, cannot confer Article III standing.

And I know Your Honor knows this, but I think it's worth pointing out here that unlike in the vast majority of data breach cases Mr. Siegel has been involved in and I've been involved in and others in this room have been involved in, the perpetrator here is in custody. Her electronic devices have been seized. The stolen Capital One data has been recovered and remains in the custody of the FBI. Critically, there's no evidence that the stolen information has been disseminated or misused in any way.

I think maybe the most important -- I mean, just a key, key fact is, you know, they rely on this purported expert, Kevin Mitnick, the former criminal hacker who -- I don't know if they knew this or not before his deposition, but he blurted out in his deposition that he had looked for the Capital One data on the dark web but couldn't find it. And you don't have to take my word for it. We have the clip, and

it's really worth watching. It's two minutes at the most.

THE COURT: Go ahead and play it. I've read the transcript. Go ahead.

(A video is played.)

MR. BALSER: That's their expert, not ours. They looked. They couldn't find it. The evidence here shows nothing more than a mere compromise of the data, which under *Beck* is insufficient to afford standing. If plaintiffs' data was not disseminated, it could not have been used to commit a fraud.

But I think to Your Honor's point, you know, a few minutes ago, even if the plaintiffs had evidence that Thompson disseminated the stolen data, plaintiffs could not establish standing based on some unspecified risk of fraud in the future. I think that's what *Ramirez* holds. That risk-based theory of standing is out after *Ramirez*.

Plaintiffs' only avenue for establishing standing would be to prove that they suffered identity theft traceable to the cyber incident, and the record conclusively shows that the frauds that the plaintiffs alleged were not committed with Capital One data.

The second standard -- and I know the Court is familiar --

THE COURT: Mr. Siegel centrally disputes that. He says that there is sufficient evidence from which the inference of traceability can be made.

MR. BALSER: We'll look at it. We'll look at it for each plaintiff very quickly.

THE COURT: All right.

MR. BALSER: I don't want to belabor it, but we'll go through them one by one.

THE COURT: All right.

MR. BALSER: The second thing that Article III requires is traceability. The traceability inquiry here completely debunks the plaintiffs' claims of actual identity fraud.

The Fourth Circuit held in *David v. Alphin* that Article III requires a fairly traceable connection between the alleged injury-in-fact and the alleged conduct of the defendant. We've already talked about *Hutton*. I'm not going to rehash the facts there, but I think the most important part of the *Hutton* holding is the traceability portion of that opinion where the court permitted standing on the 12(b)(1) challenge because the allegations were that the defendant was the only common source that collected and continued to store the exact information that was required to commit the fraud that the plaintiffs experienced.

Thus, here, to prove that actual fraud was traceable to the cyber incident, which post *Ramirez* is the only way plaintiffs could have standing to seek damages, plaintiffs must show that the stolen data has already been misused and that the instances of fraud that they claim to have suffered could have been committed using the data stolen in the cyber incident.

Seven of the eight representative plaintiffs here claim to have suffered actual fraud as a result of the cyber incident. As an initial matter, for the reasons I've already discussed, these frauds are not traceable to the cyber incident because the data was not disseminated. If Thompson herself didn't commit fraud and there was no dissemination, then the data, obviously, cannot be used to commit fraud.

Moreover, as we explained in our motion and I'm going to go through in a minute, Your Honor --

THE COURT: The one that hasn't is Hausauer?

MR. BALSER: I'm sorry?

THE COURT: The plaintiff that hasn't claimed actual fraud is Hausauer?

MR. BALSER: Correct.

Each specific instance of fraud alleged by plaintiffs would have required data that was not exfiltrated in the breach.

So I promised you we would do this. Let's look at each plaintiff:

So Brandi Edmondson alleged that there were Amazon charges placed on her Capital One card and that she had unemployment benefits filed with the Texas Workforce Commission. In order for those frauds to have occurred, she would have needed to have credit card information and a social security number exfiltrated in the breach, but that information was not stolen as to Ms. Edmondson.

Next, Plaintiff Emily Gershen. Her alleged fraud was attempted account openings at various banks and an attempt to transfer money from her Charles Schwab account. Again, social security number and Charles Schwab information which were required to commit that fraud were not stolen in the cyber incident.

THE COURT: So what establishes the need for the social security number in the record?

MR. BALSER: I'm sorry, Your Honor. Oh, that's identity fraud. So in order for someone to take over someone's identity and attempt to open a new account, you would have to have their social security number.

THE COURT: That's reflected where in the

record? Is that in an affidavit, or is that in testimony?

MR. BALSER: I can find a cite for Your Honor. My team will help me do that.

THE COURT: All right.

MR. BALSER: Sara Sharp, she alleged that she had a $100 debit against her account and that a Kohl's account was opened in her name. Again, the information necessary to commit those frauds was not stolen in the cyber incident.

Mr. Spacek alleged fraudulent activity on his BB&T account. That activity occurred prior to the cyber incident and, of course, could not be traceable to the incident since it occurred before the cyber incident.

Caralyn Tada, she alleges attempted and successful fraudulent charges on her credit union account and accounts opened at various retailers. Again, the information necessary to commit those frauds was not taken in the data breach, not stolen as to Ms. Tada.

Gary Zielecke alleged a problem with his phone number, attempted charges on his Capital One card, and a line of credit opened in his name at Synchrony Bank. Again, the information necessary to

commit these frauds was not stolen in the cyber incident.

And as Your Honor noted, Brandon Hausauer does not even claim identity fraud that would be traceable to the breach.

So, again, when you look at this, the only people you can look at are people who sued us, the eight people who are representative plaintiffs here, and none of these people has suffered a fraud that's attributable, directly traceable to the cyber incident. Accordingly, they cannot show injury or traceability, and they have no standing.

So facing these headwinds, plaintiffs offer several legal arguments and factual arguments, none of which is persuasive. I want to start with the legal arguments, and I'm going to briefly address the factual arguments. Your Honor picked up on several of those earlier today.

The first argument -- they argue four things. They argue that Olsen's access theory of injury does not depend on dissemination. So it doesn't matter if the data wasn't disseminated under Olsen's theory. They argue that they have standing because the data could have been enriched, and that's Mitnick's opinion. They say they have standing based on incurrence of

their mitigation expenses, and they argue that they've shown a risk of imminent harm sufficient for injunctive relief.

So let's start with this access theory of Olsen. What plaintiffs argue is that, based on Mr. Olsen's opinion, plaintiffs should be awarded the value of Paige Thompson's access to their data. They argue that -- and I quote, this is from their brief -- that the plaintiffs were injured the moment the hacker exfiltrated their PII.

But equating access with injury is no different than equating the mere compromise of plaintiffs' personal information with injury, which the Fourth Circuit has squarely rejected in *Beck* and *Hutton*, which we've discussed extensively. To reiterate, those cases hold that mere compromise of data is not an injury-in-fact. This forecloses plaintiffs' argument that they were injured at the moment of Thompson's access.

The logical extension of plaintiffs' argument about Olsen's theory is that plaintiff would always have standing to sue for a data breach. No court has accepted that position.

Their second argument is that the possible enrichment of plaintiffs' data can confer standing.

But as a matter of law, Mr. Mitnick's enrichment theory is not traceable to the cyber incident because it relies on data that's not stolen from Capital One. That theory requires several compounding speculative assumptions.

There's really four of them. The first assumption is that the stolen data is available to bad actors, but that's contrary to all record evidence. The second assumption is that a bad actor would target one of these eight plaintiffs as opposed to one of the 98 million other putative class members, and then that the bad actor would commit an intermediate criminal offense to enrich that plaintiffs' data and then that the bad actor would misuse the enriched data to commit fraud that causes harm to these plaintiffs.

The *Clapper* court had a great quote I think is apt here. They said that this is a highly attenuated chain of possibilities that the Supreme Court held in *Clapper* fails to establish standing.

There's a great quote in the Third Circuit case of *Reilly v. Ceridian Corporation* -- this is a data breach case -- where the Third Circuit found that there was no standing. And what they said in that case was similarly, we cannot now describe how appellants will be injured in this case without beginning our

explanation with the word "if." If the hacker read, copied, and understood the hacked information and if the hacker attempts to use the information and if he does so successfully, only then will appellants have suffered an injury.

So too here. It's impossible to trace plaintiffs' allegations f actual fraud to Thompson's stolen data without a similar string of hypothetical ifs. As a result, plaintiffs' enrichment theory cannot meet the traceability test. Moreover, enrichment would show, at most, that plaintiffs were at risk of identity fraud in the future, which, as we discussed, is insufficient for standing after *Ramirez*.

We've talked about mitigation expenses some, but we haven't talked about their new theory about mitigation expenses, which is they argue that mitigation expenses alone can constitute an injury-in-fact as long as the perceived risk of harm was objectively high at the time they were incurred. That is a construct created by the plaintiffs. That's not the law.

In *Clapper*, the Supreme Court held that where the harmed plaintiffs seek to avoid is not certainly impending, any cost incurred as a reasonable reaction of that risk of harm cannot confer Article III

standing. No court has adopted plaintiffs' hindsight theory of mitigation damages, and the theory is further undermined by *Ramirez*, which limited *Clapper* to the context of injunctive relief only.

THE COURT: This gets back to my earlier comment and question; that is, from your perspective there's no level of future risk absent materialized harm that would satisfy standing after *Ramirez*?

MR. BALSER: I don't think so. I think the answer is no. I think that it has to materialize or it has to create another harm that was identified in *Ramirez* as a common-law harm that could support standing.

THE COURT: But what if in this case -- and this is making up facts that's not in the record. But let's say the evidence was Paige Thompson, instead of saying what she did, she said, Before you got me, I was able to exfiltrate it out. There are any number of people that have it out there, people who I know want this information. I would expect they're going to use this information.

Instead of Mitnick saying his people couldn't find anything, he says, I went on the dark web. It's out there. I can find it. If I wanted to use it malevolently, it would be an easy thing to do.

Do you think those kinds of facts in the absence of an actual materialized harm would be enough?

MR. BALSER: I don't think for a damages claim it would.

THE COURT: Well, for standing.

MR. BALSER: I don't think it would -- I don't think that would rise to the level of standing for a damages claim. It might change the calculus on imminent risk of harm for injunctive relief. I think if you read *Ramirez*, just the plain language of *Ramirez*, I think a risk of harm has to materialize and become concrete before it can support a claim for damages.

Again, it's -- of course, those aren't our facts, and I think your hypothetical is certainly, you know, different. It would be a little more challenging, but those aren't our facts. But even under those facts, unless the harm is concrete and particularized and it's materialized, that wouldn't be enough.

Now, in your hypothetical, if, for example --

THE COURT: Let me ask: During that interim situation from the risk until something has materialized, are the statutes even operating, the statute of limitations? So that if somebody five years

out can prove -- ten years out can prove that their identity was stolen and it's reasonably traceable back to this data breach in 2019 --

MR. BALSER: It's a great question. It would depend on each state. I think accrual statutes on when a statute begins to run, whether it's first notice of potential harm or whether actual injury, would create the accrual. So I don't -- I think it would depend.

Coming back to your hypothetical, I think there are ways, for example, that standing for damages could occur in your counter-factual hypothetical on this -- it's out there and everybody knows it's out there, but nothing has happened yet. If someone, for example, alleged some kind of emotional distress as a result of that, which isn't alleged here, I think that is the kind of harm that could support standing under *Ramirez*. But for a claim for damages for misuse of the information, I don't think the fact that it's out there but not yet misused would support standing for a claim for damages under *Ramirez*.

THE COURT: All right.

MR. BALSER: So let's talk about injunctive relief. Post *Ramirez* plaintiffs' risk of future harm argument can, as a matter of law, only support standing to seek injunctive relief. This is what we were just

talking about. But they can't meet that standard here.

Under *Griffin v. Department of Labor*, which is a Fourth Circuit case from 2019 that we cite, the Fourth Circuit said that an injury should be certainly impending to serve as the basis for standing and to sue for injunctive relief.

In *Beck*, interestingly, the Fourth Circuit held that there was no standing to seek an injunction even though the defendant hospital in that case had suffered at least 17 data breaches after the 1 that gave rise to the plaintiffs' lawsuit. The court there said that the most that can be reasonably inferred is that plaintiffs could be victimized by a future data breach.

To get an injunction, plaintiffs have to show a sufficient likelihood that they will, again, be wronged in a similar way. Plaintiffs can't even prove that they've been harmed by this breach, let alone that they're at imminent risk of suffering harm from another one. And so they shouldn't -- the Court should find that they don't have standing to assert an injunction claim.

So none of plaintiffs' legal arguments hold up. So now what do the plaintiffs resort to? With the law clearly against them, they've attempted to create

several factual disputes based on things like Thompson's social media posts, these grassy knoll second shooter theories, and other outlandish speculation.

They try to create several factual disputes. I would start -- I do want to touch on them because Your Honor had focused on those and asked Mr. Siegel some questions about them this morning. But I will note at the outset: Based on the charts that we looked at with respect to each of those plaintiffs, it doesn't matter. I mean, they could have a factual dispute on some of these, but it wouldn't be one from which a jury could conclude that any of these plaintiffs suffered a harm that's directly traceable to the data breach for all the reasons we looked at with respect to each of those.

My team has given me the answer to Your Honor's question. Exhibit 11 to our standing motion, which is the supplemental report of Rebecca Kuehn, K-U-E-H-N, at pages 20-23 goes through each plaintiff and addresses the data that would be needed for those harms to have been committed.

THE COURT: All right.

MR. BALSER: So let's talk just very briefly about these factual disputes.

Thanks, Guys.

So the first is she shared information on Twitter. I do want to correct one misstatement that Mr. Siegel made this morning. She did not put the exfiltrating information on GitHub. What she put on GitHub were purported instructions on ways to attack our website, not the data itself was loaded there.

So she made all of these statements about what she might do and what she could do.

THE COURT: So it wasn't instructions on how to access the data that she had taken separate and apart from hacking the system again?

MR. BALSER: She shared the instruction on how to download the S3 buckets from Capital One's cloud.

First, I'd say all the statements are inadmissible hearsay. But in any event, those statements show, at most, that Thompson thought about disseminating the data, had ideas about disseminating the data, but no jury could reasonably conclude from only those statements that Thompson did, in fact, disseminate the data.

THE COURT: This is between March and July, right?

MR. BALSER: That's right.

Let's talk about the criminal case. Plaintiffs point to several facts that, at best, invite speculation into what Thompson might have done or might do. They say that the data was in a format that was easily searched and readable. They say her trial has been continued five times. The government's investigation is continuing. She's got a cell phone, and she's out on bail. And they point to the superseding indictment, which we'll talk about in a minute. But none of this shows that Thompson used the data for fraud or that plaintiffs are at imminent risk of harm, which post *Ramirez* can only give standing for injunctive relief anyway for the reasons we've talked about.

So let's talk about the superseding indictment because Mr. Siegel mentioned that this morning and alluded to it. I think it is important and interesting to look at: What did happen in the superseding indictment? We have this on the slide. The superseding indictment actually underscores that plaintiffs lack standing.

So they've now been investigating her crimes for nearly two years, and they've charged her only with possession and attempted use. They have not charged her with actual use, only possession, and we knew that

from the beginning, that she possessed it. But if the government could have proven that she used it or transferred it, they would've, and they only allege that she possessed it, again, which we've known. So there's nothing new there other than they brought enhanced charges, but they didn't charge her with use or transfer, which would have given them enhanced penalties if they had been able to prove it.

So let's talk for a second about Mr. Mitnick and the burden. I heard Mr. Siegel say today, this morning, that plaintiffs said we can't prove that the data wasn't disseminated, but it's not our burden to show that. It's their burden to show that they have standing.

You know, they now try to characterize Mr. Mitnick's search as inconclusive or superficial, but no matter how they characterize his search, he didn't find any evidence of it on the dark web. And plaintiffs, in their own words, can only speculate that others may have the data even if it's not on the dark web. And under *Ramirez*, that's just not enough to confer standing for a damages claim.

In addition, I heard Mr. Siegel say something this morning about Mr. Mitnick opining that the plaintiffs here had been injured. But in addition to

lacking any evidence of dissemination, Mitnick also made clear in his deposition that he is not offering any opinions on whether any of the representative plaintiffs suffered any specific incident of fraud or identity theft as a result of the cyber incident.

Again, as Your Honor has repeatedly questioned today, the issue isn't just injury. It's also traceability, and they have no evidence of either.

I am not going to spend a lot of time on this second intruder theory, but they assert this, what we call the grassy knoll theory. It's a disputed issue of fact as to whether Thompson was the sole attacker. They have absolutely no evidence, zero evidence, that there was a second intruder. They haven't even conducted their own forensic investigation. Rather, the so-called disputed evidence that they point to is actually the absence of evidence. They say there's no way to be certain that there wasn't another intruder given the absence of some of the ModSec WAF logs. But this is based on plaintiffs' and Dr. Madnick's misunderstanding of logs with which he admitted he had no experience.

In fact, Capital One maintained a comprehensive set of logs, which are called the Cloud Trail logs. Capital One indefinitely retained those

Cloud Trail logs, and they are duplicative of the ModSec WAF logs. The ModSec WAF logs would not have shown any additional exfiltration activity that's not reflected in the Cloud Trail logs. The Cloud Trail logs were sufficient for both Capital One and Mandiant to conduct a forensic investigation, and that investigation showed that Paige Thompson was the only intruder. Plaintiffs cannot create a fact issue by speculating about what the evidence does not show.

They also suggested earlier this morning that this data was openly accessible to anyone from the Internet. That's not true. I will point the Court to the expert report of Mr. Art Euhan, E-U-H-A-N. The data was not open to the Internet.

They didn't say much this morning -- although, they did in their papers -- about some theory that this was an inside job as opposed to Paige Thompson. But there's no evidence that there was a second intruder either inside or outside of Capital One. And, again, it's not our burden to prove that there wasn't a second attacker. Plaintiffs have no evidence from which a jury can conclude that anyone other than Paige Thompson accessed the data.

We've already talked about enrichment. I'm not going to repeat the arguments that I've made. I'll

only note that Mitnick also admitted in his deposition that there's no evidence that any plaintiffs' data actually was enriched here. There's no evidence that Thompson or anyone else actually enriched the data. It's pure speculation that's insufficient to support standing.

They raise factual issues about remediation. The plaintiffs say that there are hotly contested factual disputes, but they don't say what those are. But the uncontroverted record evidence shows that Capital One immediately remediated the root causes of the cyber incident. And in addition, they comprehensively improved its security practices under the continuing oversight of its regulators.

In any event, under *Beck*, *Beck* requires an imminent risk of a similar harm, which plaintiffs here cannot show. And it's undisputed that the misconfigured WAF that led to the breach has been remediated. So none of plaintiffs' factual arguments have any merits.

Even if there were -- again, back to this *Ramirez* problem. Even if there were a kernel of truth to these disputes -- and there's not -- there's still not enough to give plaintiffs standing. These factual disputes would show, at most, that there's a future

risk of fraud, which after *Ramirez* is gone as a theory of standing.

Plaintiffs would still be required to demonstrate that they have suffered actual fraud that's traceable to the cyber incident, and they just can't do that. None of the eight representatives plaintiffs can show with evidence that they suffered an actual fraud as a result of the cyber incident.

So in conclusion, when you read *Ramirez*, *Beck*, and *Hutton* together, it's clear that Article III requires a concrete, nonspeculative injury that's traceable to conduct of the defendant in order to confer standing. Risk of harm is insufficient. Speculative inferences are insufficient.

And because plaintiffs have not provided evidence of concrete, nonspeculative injury, this Court should dismiss plaintiffs' negligence claim, the state statutory claims, and their claims for injunctive relief for lack of Article III standing.

I think that provides a really good framework for us to dive into the class cert arguments. I mean, unless the Court has further questions about standing, I would like to turn now to responding to plaintiffs' motion for class certification.

I think the standing arguments -- and I'll

explain how right upfront -- can and should, should the Court agree with us on our standing arguments, makes the Rule 23 job much, much easier. I'll kind of walk the Court through why I say that.

I think the place to start, Your Honor, on plaintiffs' motion for class certification is to look at where the plaintiffs started and where they are now. Plaintiffs filed their complaint in this case primarily pursuing claims of negligence which they alleged resulted in monitory damages that would flow from the misuse of their personal information that was stolen in the cyber incident. That's how the complaint is framed up.

After nearly two years of litigation and extensive discovery showing that no such injuries materialized, plaintiffs have pivoted to a claim that Capital One somehow breached a contract, based upon statements in its privacy notices, causing alleged damages to the class that are untethered to any misuse of the stolen information or in the data breach itself.

Plaintiffs' new theories of injury fair no better than the ones that they've abandoned. Their claims are legally deficient. They're based upon speculative and inadmissible expert testimony. And for the reasons I'm going to talk about now, they're wholly

unsuitable for class certification.

We struggled mightily to figure out the best way, the most efficient way to present these arguments to Your Honor. It's -- you know, their motion covers a lot of ground. Mr. Siegel had 170-plus slides. We think the best way to approach it is to really focus on their theories of injury.

To set things up, I think it makes sense to just remind the Court what it is the plaintiffs are seeking to certify. So they're seeking certification of a nationwide 23(b)(3) damages class under claims for breach of contract, negligence, and unjust enrichment. They're seeking certification of four state statute-specific subclasses under the California Unfair Competition Law, under the California Consumers Legal Remedies Act, under the New York General Business Law, and under the Washington Consumer Protection Act. They're seeking certification of a nationwide 23(b)(2) injunctive relief class and, alternatively, they're seeking issue certification on elements of duty and breach.

I want to start by orienting the Court to the standards which I know the Court is familiar with, but I think it does make sense to think about first principles here and what we're doing.

Class actions are an exception to the general rule that a party in federal court may vindicate only his own interest. That's the *Thorn v. Jefferson-Pilot* case. Plaintiffs bear the burden to affirmatively demonstrate their compliance with Rule 23. That's the *Wal-Mart* case. Plaintiffs also bear the burden of establishing that damages are capable of measurement on a classwide basis. That's *Comcast*. The Court must conduct a rigorous analysis of plaintiffs' motion. That's *Thorn*. As part of that rigorous analysis, the Court has to make findings on whether the plaintiffs carried their burden of demonstrating compliance with Rule 23. And *Wal-Mart* also teaches that a class cannot be certified on the premise that a defendant will not be entitled to litigate its defenses to individual claims.

Now, before I jump in to the Rule 23 morass, the rubric that we have to work our way through, I want to explain upfront the relevance of the other pending motions to the question of class certification. Plaintiffs' motion for class certification does not exist in a vacuum. There are several other pending motions that relate to and inform the Court's analysis here. The Court, I think, correctly noted that when asking us to address standing in tandem with the class

certification inquiry. It's appropriate.

And the way the Court rules on those other motions may greatly simplify the work that's necessary to conduct the rigorous analysis that's required under Rule 23. For example, let's take a look at what -- so this is a list of all -- what I've got on this chart, Your Honor, is a list on the left side of all the claims that the plaintiffs are seeking to certify, and on the right a list of the alleged harms that they say correspond to those claims.

THE COURT: Before we get to that, tell me what's your position and where we are on Article III standing with respect to the breach of contract claim.

MR. BALSER: As I'm going to explain in a few minutes, I think the -- and we'll see this as I go through this chart. I think where we are is that the Court agrees with us on our standing arguments. The theories --

THE COURT: On the Article III standing with respect to negligence, statutory claims, and unjust enrichment?

MR. BALSER: Right. But part of our argument on standing is that these claims for increased risk -- like submitting this claim of increased risk is not a viable theory. And the market value theory that

measures a noninjury is not a viable theory that can confer standing. We think that if you agree with us on those and that those theories of damages are out of the case either on standing analysis or under *Daubert*, which we'll talk about in a minute, then I think what you're left with on breach of contract --

THE COURT: But those are damages methodologies, correct? Those aren't injury methodologies.

MR. BALSER: That's right. I think on injury they've alleged that -- and we don't think they can prove, but they have alleged that they've suffered these harms of, you know, disgorgement, increased risk of harm and market value, for example, to support their breach of contract claim. They claim those are injuries. We don't think those are requisite injuries.

So we think, really, everything would be -- I mean, if the Court accepts our argument, as I think it should, that you need a real injury to support a claim for nominal damages, then I think the breach of contract claim would also be gone for certification purposes. Because absent injury, you can't have nominal damages. And we say these speculative theories of increased risk in market value are not injuries that are cognizable for purposes of standing. So I think

that's where we would be left if the Court accepts our arguments on standing.

THE COURT: But isn't that the same as arguing that there's no Article III standing as to the breach of contract claim?

MR. BALSER: It is. I think it is. In effect, it is. The only difference is that when -- when we raised this motion, you know, we didn't have before the Court all of these arguments we have on market -- we didn't have *Ramirez*, and we didn't have the market value and disgorgement theories completely teed up. But I think the logical extension of the arguments that we make is that without injury, there's no standing. You've got to have injury to get even nominal damages.

THE COURT: All right.

MR. BALSER: So that's kind of where I was going, right. So if the Court finds that there's no standing, then I think the negligence injunctive relief and the state statutory claims are gone. If the Court grants our *Daubert* motions, that would provide additional independent bases to eliminate the theories of injury that underlie these claims both from Olsen and from Mitnick and Long, which are based on, you know, the increased risk theory.

Then you would be left with the question of in the absence of injury, can you award nominal damages? And the answer to that is no, and that's the basis of our summary judgment motion that's pending -- part of the basis for our summary judgment motion that's pending.

THE COURT: Right. Doesn't that go to the merits rather than certification in the sense that --

MR. BALSER: It does.

THE COURT: -- the issue is whether there's a common damages methodology that plaintiffs want to apply classwide that can be adjudicated on a classwide basis that has a common answer as to all members of the class? Now, it may prove that the damages theory doesn't hold up on the merits.

MR. BALSER: There are many reasons --

THE COURT: That could be decided within the context of a certified class if we get that far.

MR. BALSER: Well, there are many reasons that we'll talk about why these damages theories can't satisfy Rule 23. So I think it's not just a merits issue. It's whether these theories -- and really, they're traveling under three main theories, the market value theory, this increased risk of harm theory, and disgorgement.

THE COURT: Right.

MR. BALSER: And that's how we've really tried to organize the argument because I think that's really the organizing principle here, to look at what they're claiming, what relief they're seeking. And when you pull those apart and analyze them, I think they have -- there are a host of gating and threshold problems with them. But just on a pure Rule 23 predominance analysis, they fail, and I'll explain why.

THE COURT: All right.

MR. BALSER: Okay. So the point I'm trying to make is that there are numerous gating issues that are raised in our other motions that have the potential to significantly narrow the claims and the injuries that are relevant to class certification. That's the point.

And those motions should be decided before the Court rules on class certification. Of course, we haven't argued the *Daubert* motions yet. So I'm going to proceed today under the assumption that these claims and injuries are all properly considered for purposes of certification even though for the reasons I've explained in the standing argument, I think, you know, most of them should be out, the vast majority of them.

So I will touch on those other issues that

are raised by the other pending motions as appropriate in the course of my argument. And again, I'm happy to focus on and address any issue the Court has an interest in, but I plan to cover the following points.

I want to start with a very brief summary of the relevant facts. I know the Court is very familiar with the record. I want to talk just briefly about standing through the lens of Rule 23. We talked about essentially the merits of the standing problems, but there's some Rule 23 issues as well. I want to address each of the plaintiffs' injury theories, the increased risk theory, the market value theory, and disgorgement primarily to explain how they fail to satisfy the predominance requirement of Rule 23(b)(3). Then I want to have a very brief discussion of nominal damages since Mr. Siegel spent some time on that this morning. Then I want to briefly cover some additional barriers to class certification for plaintiffs' claims for breach of contract, unjust enrichment, and violations of the state consumer protection statutes. Then very, very briefly I wanted to hit on injunctive relief, issue certification, and superiority.

So real quickly on the facts, this Court knows the data stolen in the cyber incident largely consists of nonsensitive information that consumers

submitted to Capital One when applying for credit cards. There are 98 million putative class members. The putative nationwide class includes both applicants and cardholders -- we'll talk about that -- who applied for credit over a 15-year period from 2005 to 2019.

Importantly, Your Honor -- and we tried to explain this in our papers. I'm not sure, but I hope we did a good job of it. But during this 15-year period, consumers applied for different Capital One credit cards using many, many different applicant channels, and they received a variety of different documents along the way doing that. And those differences in the methods of applications are significant here.

Plaintiffs have asserted that each applicant was provided with Capital One's privacy notice when they applied, but that's not true. The disclosures, notices, and information provided to applicants varied over time and by channel. If you look at this slide that we have up, this is a description of the application channels for Capital One branded cards. It's all the different channels through which someone could apply on the left and then the manner in which the privacy notice was or was not delivered with respect to each of those Capital One branded cards.

And then another layer of complexity here is that some of the putative class members did not apply to Capital One for credit at all. They, instead, applied through other entities that were later acquired by Capital One, or they applied to our retail partners. So if you look at the slide that's up here, this is the application channels for our partnership cards. So not Capital One branded cards but partnership cards. And again, there are different channels. And the privacy notice was either not provided or provided optionally through a request to click, but all in different manners through the different channels.

Now, look, as the Court knows -- I'm not going to belabor this on the privacy notice, but of course, the Court is aware that the content of the privacy notice itself changed during the putative class period. Before 2010 -- after 2010, it included the language that says security -- we have security measures that comply with federal law. The privacy notice before 2010 did not include that language.

Turning to the cyber incident itself, the Court knows we discovered Paige Thompson's theft of the impacted data in July of 2019. Capital One worked with law enforcement to identify her and aid in her arrest. Since that cyber incident occurred, Capital One has

remediated all of the factors that led to it and made comprehensive improvements to its cybersecurity defenses.

Capital One also offered free credit monitoring to anyone whose information was stolen. Mr. Siegel asked why did we do that: Why would Capital One have done that? There are a couple of reasons. One is several states data breach notification statutes require a company that's a victim of a data breach to provide credit monitoring. And also, Capital One wanted to let its customers know that even though, under the best evidence that we had, the data was not out there, we wanted them to have this service and show that we were concerned about them and cared about them.

THE COURT: So all 98 million were offered the data monitoring?

MR. BALSER: Yes.

THE COURT: For how long?

MR. BALSER: Yeah. They didn't all get an invitation in the mail. But, yes, it was open -- in fact, not only was it open to the 98 million people, it was actually open to any U.S. citizen. So even if you were not a victim of the data breach, you could have signed up for free credit monitoring through --

THE COURT: How many people signed up?

MR. BALSER: I don't know if I have the exact number. It may be in our papers, but that's, you know, really kind of an interesting issue. Not very many, and that kind of goes to -- that actually bears on some of our arguments on the claim for unjust enrichment, whether plaintiffs really -- you know, how much they care about the fact that there was a data breach, especially when the data hasn't been disseminated. But there was not a huge uptake. A very small percentage of --

THE COURT: How long was the monitoring offered?

MR. BALSER: At least two years.

Is it still in place?

It's still open. I mean, you can still enroll. You can enroll today.

THE COURT: All right.

MR. BALSER: So as I mentioned before, the vast majority of the stolen data was nonsensitive information, like names, addresses, phone numbers, dates of birth, self-reported income that could not be used to commit fraud or identity theft. Less than .2 percent of the putative class had social security numbers or bank account numbers taken. So 99.8 percent of the class did not have social security numbers or

bank account numbers taken.

And we point this out in our papers, and this is important. I'm going to come back to it. The data combinations that were stolen by Paige Thompson are extremely diverse. There are over 724 different unique combinations of data elements presented with respect to the 98 million people in the class.

Look, the representative plaintiffs themselves illustrate the variation across the impacted data elements. For example, Plaintiff Brandi Edmondson did not have any identifying information stolen, such as her name, address, or date of birth. Rather, her anatomized credit information was stolen, and Capital One was only able to link that information to her based on her own internal account ID number.

On the other hand, Plaintiff Hausauer is part of the .1 percent of the putative class who had his social security number stolen. His name and date of birth were also stolen, but he doesn't allege identity theft. So, you know, the harms alleged, you know, also vary. Ms. Edmondson and four other plaintiffs claim they had an unauthorized charge on their credit or debit card after the cyber incident even though no card numbers were impacted in the breach at all, none, zero credit card numbers. But Mr. Hausauer and another

plaintiff, John Spacek, don't allege any misuse of their information at all after the data breach.

Okay. I've got the answer on the credit monitoring.

THE COURT: All right.

MR. BALSER: Two years credit monitoring was offered. It's still open, but you would get two years if you signed up. Less than 1 percent of the class signed up for credit monitoring.

In addition, every single named plaintiff was impacted by at least one data breach before the cyber incident. This is a chart that shows that fact. So when you look at this, John Spacek was the victim of six different data breaches; Brandi Edmondson, six different data breaches.

THE COURT: These are all before March 2019?

MR. BALSER: All before March 2019.

You know, many of them were victims of *the Equifax* data breach, several of Yahoo and Marriott.

And so the point is that -- you know, kind of getting back to this traceability issue, you can see -- and this kind of goes to this -- the slide that Mr. Siegel showed you earlier on the concurrent cause. You know, jury charge under Virginia law. I mean, in order for there to be a concurrent cause, both causes

have to have been shown to be potential proximate causes. As we looked at when we went through each of the named plaintiffs, none of their fraudulent charges are traceable to this data breach. But you look at the fact that there's all of these other data breaches that affected their data, and you can understand how fraud could occur. It's just not traceable to our breach such that a concurrent cause kind of -- a jury instruction would be appropriate here.

Beyond that, beyond just the named plaintiffs, we sought discovery from plaintiffs named in the member complaints that are consolidated in this MDL. And of the 99 member plaintiffs who answered -- most of them dismissed their complaint when we asked them for discovery -- nearly half were impacted in prior data breaches, and nearly 20 percent of those were victims of identity theft before the cyber incident.

So these findings, when you apply them to the putative class more broadly, suggests that the vast majority of the proposed class has also been the subject of at least one prior data breach.

Finally, discovery also revealed ways in which plaintiffs' data is accessible to third parties completely unrelated to the cyber incident, including

by voluntarily making their information available in the public domain, generally for free on social media, Facebook, LinkedIn, and the like, public record searches, and the like.

So that's just a real brief overview of the facts. I know the Court is familiar with them, but I wanted to just kind of set the stage here.

I want to talk just real briefly about the Rule 23 implications of the Article III standing discussion that we had. Article III standing issues create serious problems for the plaintiffs on class certification completely apart from the merits issues that we discussed in two key respects.

As I'm going to talk about in some detail, plaintiffs' market value and increased risk theories of injury fail under Article III. *Beck* and *Hutton* foreclosed Olsen's market value theory, which is mere access, which is just like mere compromise of data provides some injury. That's the claim. That's foreclosed by *Beck* and *Hutton*.

And *Ramirez* clearly forecloses Mr. Mitnick's increased risk theory, which is the basis of Mr. Long's exorbitant $838 billion calculation present value of damages to guard against that increased risk, which is not a theory of damages that's now cognizable under

Article III and, therefore, certainly couldn't support class certification.

So, you know, where does that leave us? I think it means that the negligence and state statutory claims are out. We do need to talk about disgorgement damages, and we need to talk about nominal damages, which we will. But I think this highlights the importance of the Court ruling first on Capital One's standing challenge because I do believe it could, if the Court agrees with us, and would significantly narrow the class certification issues.

Setting aside -- like even if the Court didn't agree with us on what *Beck* and *Hutton* hold and require as to this market value theory or with our arguments that *Ramirez* forecloses the increased risk theory, the Article III standing issues also impact the Rule 23 analysis because *Ramirez* made clear that every class member, every class member has to have Article III standing in order to recover individual damages.

And *Ramirez* also confirmed that the Court can't simply presume concrete harm to absent class members. Plaintiffs have to present evidence to factually establish each class members' harm, which was totally lacking for the approximately 6,000 class

members in *Ramirez* found not to have standing.

So that means to get a claim for damages certified, plaintiffs have the burden of showing how they will establish with common evidence concrete harm for each of the 98 million class members, and they can't do that. They have completely failed to meet their burden in that respect.

But even if you accepted those injuries, that is, the market value injury and the increased risk injury as legally viable, plaintiffs have put forth no method for proving those injuries for each class member using common classwide evidence. Rather, proving each of plaintiffs' theories of recovery across the putative class would require millions of individual mini-trials.

Why do I say that? Let's just think about a couple of examples. Plaintiffs have no way of determining on a classwide basis which class members' PII was already exposed or publicly available. Plaintiffs have no way of determining on a classwide basis which class members' application data was used by Capital One's models to prevent fraud, and plaintiffs have no way of determining on a classwide basis whether any risk of harm from the stolen Capital One data materialized into actual harm using that data.

There's not a shred of evidence for any

putative class member to prove those points, and plaintiffs haven't even tried to show otherwise. There are numerous other individualized issues that we will discuss.

So we will get into those issues in more detail, but the critical point to keep in mind is that plaintiffs have not met their burden of showing that they'll be able to prove with common admissible evidence the claims and damages of each of the 98 million class members.

And this is important. Because if any claims are certified, the Court will preside over a trial where plaintiffs will have to factually establish with common evidence the alleged injuries of each class member. *Ramirez* made that clear.

In other words, I think the Court should be thinking about what a trial on these claims would look like and whether plaintiffs have demonstrated that they can prove their claims with common evidence or whether individualized issues would make a trial practicable or really more realistically impossible.

So before discussing the numerous reasons why plaintiffs' theories of classwide injury fail to meet the requirements of Rule 23, it is important to note that the Court cannot certify any claims based upon

damages theories that are supported only by an expert, and his opinion should being excluded.

To recap, as the Court knows, we have moved to exclude all three of plaintiffs' classwide injury theories, the market value theory espoused by Olsen, the increased risk theory espoused by Mitnick and Long, and the disgorgement theory put forth by Olsen. And because the plaintiffs rely on these expert opinions in support of class certification, the Court must decide whether those opinions are admissible under *Daubert*.

And, again, I would remind the Court that our standing and *Daubert* motions have the potential to significantly narrow the claims and theories that must be analyzed for class certification, as does our motion for summary judgment which is pending. And this slide that we put up earlier, I think, shows what -- you know, if the Court rules in our favor, how simple the class certification analysis becomes if the Court goes with us on standing and *Daubert*.

So I now would like to just dive into a discussion of why the theories of injury that the plaintiffs advance can't be certified. First, I think it's important to note -- I touched on this briefly, but I think it's worthy of a little bit of focus -- plaintiffs have abandoned any chance of classwide

discovery for the vast majority of the harms that they've alleged in their complaint, including actual fraud, identity theft, lower credit scores, time spent mitigating the consequences of the cyber incident, mitigation expenses, etc. None of that is being requested as a theory of damages to be asserted classwide.

Aside from nominal damages and injunctive relief, plaintiffs now assert only three primary theories of classwide injury, which are increased risk of harm, the market value of PII, and disgorgement. So in order to obtain class certification, plaintiffs have to satisfy the Court that they can prove these theories of injury with common classwide evidence, and they fail to do so.

Now, plaintiffs have tried to reframe our opposition to these theories as involving only individualized damages calculations or challenging only whether their damages models satisfy *Comcast*, but that's not correct. We are challenging that plaintiffs can prove an injury that is proximately caused by the cyber incident under these theories.

Injury and causation are essential elements that plaintiffs must prove for all their claims, and certification depends on the plaintiffs demonstrating

that common questions of law and fact predominate over the individual questions with respect to each theory of injury that they are seeking to certify.

Let's start with the increased risk theory of harm. So just as an overview of that theory, the plaintiffs claim that all class members face increased risk of identity theft and other fraud because the stolen PII can be used to commit identity theft in the future. Plaintiffs rely entirely on their experts, Mitnick and Long, to show this purported increased risk injury.

Mitnick's opinion rests on speculation, as we've already discussed, about how bad actors can theoretically misuse the stolen data if they had access to it, including by enriching the stolen data with information available from other sources. Even though Mitnick and the plaintiffs have no evidence that the stolen data was enriched, disseminated, or otherwise misused, Mitnick concludes that all putative class members are at, his words, serious risk of ID theft, fraud, such that all of them need the same credit monitoring product, which is LifeLock Ultimate Plus, at $29.99 a month.

Then Mr. Long takes Mr. Mitnick's recommendation regarding LifeLock Ultimate Plus and

calculates the present value of purchasing that product for all putative class members leading to absurdly high damages figures ranging from $97.5 billion on the low end to $832.2 billion on the high end, sums far in excess of the net worth of the entire company.

Plaintiffs say this theory applies to breach of contract and negligence claims. We've explained in our motion for summary judgment why that theory of harm does not apply to the contract claim. But even if these were a viable measure of damages in the abstract, this theory doesn't satisfy Rule 23. So kind of putting aside whether it can survive the Article III challenge and the other merits-based problems, they've got predominance problems that can't be overcome.

As an initial matter, the theory is untenable because Mitnick's and Long's opinions are predicated on the notion that the stolen data was disseminated, but plaintiffs lack any proof that that occurred. Without dissemination, their increased risk theory is directly foreclosed by *Beck* and *Ramirez*.

Again, I don't know how many times I need to say it, but *Beck* said the mere theft of PII, without more, cannot converse Article III standing. And *Ramirez* upheld that a mere risk of future harm that never materializes cannot establish even Article III

standing; thus, it certainly cannot support certification of class.

So Mitnick does not claim that any risk is actually materialized into concrete harm. And as we've pointed out, each plaintiffs' contention of actual fraud has been disproven. But again, setting those issue aside and even assuming dissemination, plaintiffs can't prove with common classwide evidence that they suffered an increased risk of harm as a result of the cyber incident.

Why do I say that? Well, the critical thing to keep in mind here is that this theory of injury is premised on increased risk. So meaning for any given individual, the Court must first consider that individual's baseline level of risk and then assess whether the cyber incident, in fact, increased that baseline level above what it was before.

Determining whether any individual class member's baseline level of risk has increased depends on a host of individual factors, including, one, whether that individual's information has been exposed to bad actors previously; two, which specific data elements were stolen in the breach out of over 700 possible unique combinations; and, three, whether that data either on its own or in conjunction with other

data could be used to commit identity theft or fraud due to its nature, its accuracy, how old it is, etc. In addition, plaintiffs would have to show that the increase in risk is uniform across the 98 million person putative class.

These individual issues are not merely hypothetical as the facts developed in this case show. The issue of prior exposure is a huge problem for plaintiffs that they don't meaningfully address. That encompasses not only prior data breaches, as I've discussed, but the voluntary disclosures on social media, involuntary disclosures, like stolen wallets or laptops, and other forms of public available information, like public records.

Then there's the problem with the variation in the impacted data. Our expert, Professor Lorin Hitt, went through chapter and verse about the 724 unique combinations of exfiltrated data. Of course, different data elements have different sensitivity. For example, stealing someone's name and address, when for many of us are available on our Facebook accounts or Instagram accounts or LinkedIn, is much different than having a social security number taken. And, again, as our expert, Rebecca Kuehn, makes clear, the vast majority of impacted data here cannot have been

used to commit fraud in the first place.

So when you look at all of these issues about the data, including how old it is, the likelihood that some of it's not accurate anymore, it requires an individualized inquiry that's just not susceptible to class treatment. All of these factors I just discussed are specific to each individual in this 98 million person putative class.

So in order for the Court to determine whether any given class member suffered an increased risk of future harm -- that's their theory -- increased risk of future harm because of the cyber incident requires analyzing the number of prior exposures or breaches that he or she was involved in, what information had been exposed, whether that same or different information was exposed in this cyber incident, whether the information exposed in the cyber incident could be used to commit identity theft or fraud. And these inquiries go not only to damages but to the elements of injury and causation.

Another problem, despite all those individualized questions I just went through, plaintiffs propose a one-size-fits-all remedy for the entire class, which is this $29.99 a month LifeLock Ultimate Plus credit monitoring. They just completely

ignore the substantial variation I just discussed. In fact, they didn't even address the prior exposures of plaintiffs' and class members' data in their papers. They don't respond to our arguments on them.

Instead, in their reply, what they say is, Mitnick's thorough opinion concludes that all class members have been injured such that they need this remedy. And, thus, in plaintiffs' view, the extent to which plaintiffs and class members vary is irrelevant, their word.

Their reply doesn't even mention Mitnick's speculative enrichment opinion, but that's critical to their increased risk theory. So, again -- and we'll talk about this more tomorrow. I won't, thankfully, for you and for me. Somebody else will. But if Mitnick's opinion is excluded, as it should be under *Ramirez*, this theory of injury necessarily fails.

But even if you don't exclude Mitnick's opinion, plaintiffs cannot prove with common evidence that all class members, in fact, suffered the same increased risk injury in light of all of these variations that I just discussed. And as we noted in our brief, other courts considering whether to certify claims arising from data breaches reached the same conclusion.

Now, plaintiffs like to cite *Tyson Foods* for the argument that the existence of individualized damages issues don't preclude certification, but that's not the argument that we're making here. That argument is unavailing because we're challenging not just the calculations that were made, but also the injury and causation that are required elements of their claim.

So, in any event, the damages issue in *Tyson*, which centered on time spent by workers donning and doffing protective gear, is much more susceptible to a reasonable average than the raft of the individualized issues that I just went through here. And *Wal-Mart* stands for the proposition that class certification is improper where individualized determinations regarding the existence and extent of each plaintiffs' injury are required.

So unless Your Honor has any question about the increased risk of harm theory, I now would like to turn to the market value.

THE COURT: All right. Why don't we take a recess at this point. We'll take about a 10- or 15-minute recess.

I'd like to give Mr. Newby time to speak today. I don't know if you two have coordinated your time.

MR. BALSER: I'll make sure he has time, Your Honor.

THE COURT: All right. Very good.

The Court stands in recess.

(Recess from 3:37 p.m. until 3:53 p.m.)

THE COURT: Mr. Balser.

MR. BALSER: So, Your Honor, before I jump into the market value theory of harm discussion, I do want to make sure that we're on the same page about these theories of injury that I'm talking about.

So Your Honor referenced -- you asked me a question about whether these are just damages calculations that can be dealt with in some other way or down the road. The point that, I think, is important for the Court to keep in mind is this is the evidence that they are presenting of their injury. So they say, Our injury that not only gets us in the courthouse door under Article III but that can be certified is this access theory of damages or this increased risk of harm.

That's the evidence of injury that they rely on. And so the point that I was trying to make when I was talking about -- when you asked me a question, well, what's the effect, like what's left if I grant the standing motion?

THE COURT: Right.

MR. BALSER: My point about these theories of damages are that the Court can find that these are just not cognizable, not even sufficient to get them in the courthouse door, as a matter of law, just these theories themselves, which I think is the right answer, in which case you don't even have to get to the predominance arguments that I'm making. That's the point I was trying to make.

THE COURT: All right.

MR. BALSER: So it's not just an issue of calculations. It's whether these theories that they're -- this evidence of injury is all they have, whether these amount to enough to even get you in the courthouse door, much less certify class based on the theories.

THE COURT: All right. I understand.

MR. BALSER: So let's talk about the market value, the market value theory of harm. So plaintiffs have proffered the opinion of Gary Olsen, who purports to measure the market value of the hacker's unauthorized access to the PII. And he does this by comparing the stolen data to average list prices for PII that's offered for sale by criminals on the dark web and then aggregating those values across the class.

I took his deposition. Frankly, it's unclear exactly what he's measuring. But what he testified that he's measuring is -- and I'm quoting here -- the value of a one-time nonexclusive access to the PII. And that's what they say is injured. Plaintiffs say that this theory of harm applies to the breach of contract, negligence, and unjust enrichment claims.

There are a few threshold problems before we get to the predominance problems. The first problem is the Court has already rejected this theory. The plaintiffs struggle mightily to distinguish Olsen's market value opinion from their already rejected theory of harm based on the inherent value of their PII. The Court in its motion to dismiss order at page 29 said that plaintiffs do not allege any facts explaining how their PII became less valuable as a result of the breach. That was the basis upon which Your Honor dismissed the claim, but this is essentially the same theory. And plaintiffs still do not claim that class members unsuccessfully attempted to sell the data or receive less than they would have absent the cyber incident. Indeed, no plaintiff even individually makes that claim.

The second problem -- and it won't surprise you to hear me say this -- this theory is also

foreclosed by *Beck* and *Hutton*, which made clear that a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of identity theft.

So, regardless, this repackaged market value theory that plaintiffs now advance is rife with individual issues that affect the purported value of Thompson's unauthorized access, whether any class member in fact lost that value, and whether the loss is causally linked to the cyber incident. Those individual issues include whether a given individual's data was already accessible to actors, and much of the stolen data was.

It includes whether the market value of a given individual's data varies drastically depending on characteristics specific to that individual, for example, based on net worth, their credit score, occupation. There's substantial variation in the types and combination of the data elements that were stolen in the data breach. And the stolen data, much of it is outdated given that it goes back to 2005 rendering much of it now inaccurate.

So, again, these individual issues go to the core elements of injury and causation. Let's just think about a couple of examples. So if a class

members' information that was accessed by Paige Thompson was already publicly available, then that class member cannot have lost the value of unauthorized access to it as a result of the breach because it was already accessible.

To take another example, suppose that a class member applied for a credit card in 2005 but has since moved and changed her name. If Thompson accessed only her old address and former name, those data elements no longer have market value because they're no longer accurate. Plaintiffs do not even attempt to account for these kinds of individualized differences.

Olsen did not attempt to check whether any of the personal information underlying the market value theory of injury was already in the public domain or for sale on the dark web. Nor did he account for many other individual factors that affect market value despite admitting in his deposition that these were all relevant factual inquiries.

For example, Olsen didn't control for characteristics specific to each consumer such as age, occupation, creditworthiness, etc. even though he admitted in his deposition that those affect the value of the PII.

Indeed, Olsen attempts to calculate damages

by grouping the vast array of different impacted data elements -- these 724 unique combinations I've talked about -- into just four categories. He also averages the prices for which this type of data is offered despite acknowledging that prices on the dark web vary substantially. And he admits that he has no idea what the data on the dark web that he uses for his damages calculations actually sell for. There are no sale prices reflected on the dark web for stolen data, only offering prices.

So in this sense, plaintiffs' market value theory is quite similar to the approach that the Supreme Court rejected in *Wal-Mart*. Plaintiffs, essentially, are asking this Court to discard individual differences among class members and certify a class based on a statistically insignificant random, cherry-picked sampling of dark web prices offered by criminals that are averaged, grouped into categories, and then multiplied across the class.

But a class cannot be certified on the premise that a defendant will not be entitled to litigate its defenses to individual claims. That's what *Wal-Mart* tells us.

Now, plaintiffs claim that despite all of this individual variation that's inherent in this

theory, Olsen's market value analysis damages can be applied mechanistically across the data elements impacted for each class member. This argument misses our point.

Capital One contends that Olsen's formula itself is defective because it does not consider individualized factors that affect the market value, if any, of Thompson's unauthorized access to PII. For example, because Olsen does not control for information already in the public domain, he would award damages for information, like name and data of birth, that are already publicly available. And that's not hypothetical. In fact, he awards $55 million in damages to the putative class for those data elements which are available on people's Facebook page.

Not only have plaintiffs not suffered an injury based on information that's already publicly accessible, but Olsen's model independently violates the Supreme Court's *Comcast* decision by failing to measure only those damages that are attributable to their theory of liability. The theory of liability is it's unauthorized access. But if I voluntarily put my information out in the world, how is accessing that same information providing entitlement for $55 million in damages?

Plaintiffs also fail to explain how this cyber incident caused them to suffer their supposed market value injury. And this is where I think this theory really breaks down. The plaintiffs state that the market value theory does not depend on individual proof that class members would or did sell their PII. They also say that the question of whether their PII lost value is completely irrelevant to their market value theory. If that's the case, then how were plaintiffs economically damaged by Thompson's unauthorized access? They simply don't say.

I mean, this is an uneconomic harm. This is a made-up harm created out of whole cloth that they claim constitutes injury sufficient not only to get them into the courthouse door on Article III, but certify a class.

Like, what do they do? How do they try to get around that? They analogize their damages to reasonable royalties for patent infringement, but that analogy is inapt and has been rejected. The only court that has considered this same precise theory in a data breach case rejected it out of hand, and that's the *Adkins v. Facebook* case.

And my friends here, Mr. Yanchunis and Ms. Riebel, were plaintiffs' counsel in that case.

They used the same expert firm as Olsen here. They didn't use Olsen. They used his partner, Ian Ratner. And in that case, Mr. Ratner proposed the same theory that Olsen proposes here; namely, that Plaintiff Adkins was injured when unauthorized third parties got access to his personal information for free without compensation to the plaintiff. Judge Alsup in that case rejected the theory as -- and I quote -- too speculative to assert a claim for negligence. Faced with that adverse decision, plaintiffs' only response is that the *Adkins* court was simply incorrect in its ultimate conclusion. But plaintiffs are wrong, and the *Adkins* court is right.

For all those reasons, the Court cannot certify any of the claims premised on the market value theory of harm.

So now I'd like to turn to their third theory of harm that they rely on to certify a class, and that's disgorgement. This is a theory that was also concocted by Gary Olsen. As a recap, this theory proposes alleged damages of approximately $300 million to compensate plaintiffs in the putative class for Capital One's use of their application data in models to prevent fraud between 2015 and 2020.

According to the plaintiffs, Capital One

should have to disgorge the amount of fraud it prevented, that is, the benefit it allegedly obtained, by using the application data because Capital One allegedly was not adequately protecting that data.

As an initial matter, I'll just note it's somewhat odd for plaintiffs to seek disgorgement for fraud prevention which is intended to protect customers like the plaintiffs. But there are three threshold problems that I think the Court needs to consider before we get to the serious predominance problems with this damages claim:

First, as my colleagues will explain when we argue the motion to exclude Olsen, his disgorgement theory falls apart. It's neither relevant nor reliable, and the Court should exclude under *Daubert*.

The second threshold issue is -- and this is, I think, a fatal blow that the Court needs to consider, and that is that none of these eight plaintiffs can recover disgorgement damages as a matter of law. All eight of the representative plaintiffs here have entered into a cardholder agreement with Capital One, and each of those plaintiffs is asserting a breach of their express contracts related to the cyber incident. It's black-letter law that plaintiffs' express contracts with Capital One preclude an unjust

enrichment claim based on the same subject matter, and the Court held in its motion to dismiss order that this unjust enrichment claim is just an alternative to the express contract claim.

And, you know, plaintiffs' answer to that is, well, they can seek leave to add a new applicant-only plaintiff. But they haven't done that, and the time to do so is long past. They've amended twice, including to add new plaintiffs. And plaintiffs chose to proceed by representative complaint, rather than consolidated complaint. And they're the ones that chose these cardholders as their representative plaintiffs. We didn't choose them. They did.

Third and finally, plaintiffs keep saying that they can recover disgorgement damages under breach of contract claim, but they can't cite any Virginia authority to support that position. We explain in our summary judgment motion why that's wrong. But in sum, the Court should first decide whether, as a matter of law, any of these plaintiffs can recover disgorgement damages before it goes through the trouble of analyzing whether this theory of injury satisfies Rule 23, which for the reasons I'm going to explain now it doesn't.

So even if Olsen's disgorgement theory could survive these threshold challenges, the Court should

reject the plaintiffs' request to certify class claims based on this opinion.

You know, there's a lot of remarkable things that have kind of come through in the briefing here, but to me, one of the most significant ones is that the plaintiffs have conceded that their disgorgement theory is completely untethered to the cyber incident. So what do I mean by that? Their theory is premised on the remarkable notion that consumers can disgorge the profits of a company just because that company allegedly had deficient data security measures in place at some time, regardless of whether a breach occurred or any other harm was caused to those consumers. That's their theory.

If the Court were to recognize this novel theory, it would open the door to an untold number of class actions alleging that businesses that keep consumer data, like banks, healthcare companies, airlines, etc., may have at some point in time employed deficient data security measures irrespective of any harm. Setting aside that no court has accepted that theory of liability, plaintiffs fail to show how they can prove that each class member is entitled to disgorgement damages using common evidence.

To start, Olsen incorrectly assumed that all

98 million class members had their application data used in a fraud model between 2015 and '20 and that each class members' application data prevented the same exact amount of fraud, 56 cents per year. That's wrong. This fictional average of 56 cents per application is untethered to the facts of any putative class member, which fails under *Ramirez* and *Wal-Mart*. There's no record evidence to support this simplistic and incorrect assumption. Rather, not surprisingly, some data is more useful in preventing fraud than other data, and some class members' data wasn't even used in fraud models during the time period relevant to Olsen's calculation.

Determining whether any given class members' data was actually used by a model to prevent fraud during the relevant time period and, if so, how much, would require a highly-individualized inquiry, and plaintiffs don't show otherwise.

But under plaintiffs' theories, class members would be awarded damages when there's nothing to disgorge, and their data was never used in any fraud model, let alone used successfully, to prevent fraud. Plaintiffs try to dodge this issue by saying there's no evidence in the record that Capital One's fraud models couldn't function without any one individual's PII, but

that's factually untrue. As the record shows, Capital One has fraud models that function without using any application data. And it's plaintiffs' burden to prove that their damages can be established on a classwide basis and not our burden to disprove it.

And plaintiffs' position makes no sense. If a given class member's data did not result in actual fraud savings, then that class member conferred no benefit on Capital One and plainly is not entitled to disgorgement damages. Rule 23 does not permit the Court to award damages to uninjured class members. And if *Ramirez* teaches us anything, it teaches us that, because those 6,200 uninjured class members couldn't recover.

Finally, in short, Olsen's incorrect assumption that each of the 98 million class members' application data prevented the same amount of fraud is just a transparent attempt to paper over the individualized inquiries that make this theory of recovery improper for classwide treatment.

But there's another problem, and that is that the disgorgement theory fails to consider benefits obtained by the putative class, and Your Honor asked about this. You asked -- it was a perceptive question to Mr. Siegel. The law of disgorgement requires an

offset of any benefits that are received by the plaintiffs in exchange for providing their data to Capital One.

And plaintiffs try to confuse that issue by suggesting that the question is whether class members would have received benefits regardless of whether Capital One obtained fraud savings, but that's not the right question. The correct question is what benefits did class members receive in exchange for providing their data to Capital One, and the answer is that all class members received at a minimum -- and Your Honor has noted this more than once -- the benefit of having their application considered. Most class members and all the plaintiffs who are cardholders also received additional benefits in the form of credit, credit card services, and the like.

And then there's an additional question about whether any given class member benefited from Capital One's fraud prevention program specifically. So what if somebody tried to misuse your card and Capital One caught the hacker -- I mean, the fraudulent person and prevented the fraud on your account? That's some benefit. That's an individualized -- one of hundreds individualized inquires that would need to be made to figure out the offsetting benefits to calculate the

disgorgement damages that would need to be run against the 98 million person class.

But plaintiffs fail to even acknowledge these indisputable benefits, much less proposed method for determining the value of these benefits for each of the 98 million proposed class members using common evidence.

Plaintiffs testified in their depositions here of these eight named plaintiffs that they applied for Capital One credit cards for a variety of reasons proving that the value of having their application considered and a card issued would be an inherently individualized issue. Some people like the rewards program. Some people had lower credit scores, and this was the only credit card they could get. I mean, there's a wide variety of reasons and benefits that different people experience in applying for these cards, all of which would need to be taken into account to try to calculate the disgorgement theory.

In sum, plaintiffs' disgorgement theory is not capable of being proven on a classwide basis using common evidence. Suggesting otherwise, plaintiffs rely on unsupported assumptions and they ignore highly individualized inquiries that would be necessary to undertake to determine whether any given class member

can recover disgorgement damages. And while it would be convenient for the plaintiffs if each of the 98 million class members' application data benefited Capital One in the same amount of 56 cents, it's simply not the case.

And because the disgorgement theory flunks Rule 23 scrutiny, it cannot provide a basis to certify plaintiffs' unjust enrichment or breach of contract claims.

All right. So those are the three primary horses that they're trying to ride to prove injury both for Article III purposes and for certification purposes. I now want to turn to their theory of nominal damages, which plaintiffs assert is supportive of the breach of contract.

The prospect of the class recovering nominal damages for their breach of contract claim has been a hot topic throughout this litigation. Plaintiffs have suggested and they suggested again today that even if they can prove no actual harm to themselves or any of the 98 million putative class members, they could still walk away from trial with an up to $9.8 billion recovery, that is, $100 in nominal damages per class member. Mr. Siegel said it again this morning.

This issue bears on several aspects of

Rule 23, most notably the superiority requirement under 23(b)(3)(D). So it's important to understand why plaintiffs' position on nominal damages is wrong.

First -- and Your Honor was right on this this morning -- plaintiffs are wrong that the availability of nominal damages for a breach of contract relieves them of proving an injury. I think I actually heard Mr. Siegel agree with Your Honor on that this morning.

Our contracts professors in law school taught us that an essential element of breach of contract claim is actual injury, and I don't think the law has changed. It's been a while since I've been in law school, but I don't think the law has changed.

And the *Bailey v. Potter* case in the Eastern District of Virginia, I think, said it nicely. They said it therefore follows that a claim for nominal damages does not eviscerate the consequential injury or damage element of a claim for breach of contract.

Now, plaintiffs mischaracterize our argument as saying that plaintiffs have to prove compensatory damages to obtain nominal damages. That's not what we're saying. The point is that plaintiffs can't rely on a mere breach of the privacy notice standing alone to obtain nominal damages, and plaintiffs have failed

to show that they can establish an actual injury caused by Capital One's alleged breach of the privacy notice across the 98 million person class using common evidence; thus, nominal damages do not fix plaintiffs' predominance problems.

Second, plaintiffs don't dispute that they cannot recover both compensatory and nominal damages for the breach of contract claim. So if the Court rejects the classwide injury theories that plaintiffs advance and only their claim for nominal damages remains, the Court should decline to certify the breach of contract claim altogether.

And that's so for a couple of reasons. The first is, as I mentioned, these classwide damages theories are their theories of injury. That's their evidence. So if they don't have evidence of actual injury that can satisfy the Court's scrutiny that's not cognizable, then they haven't made a case for actual injury that would support an award of nominal damages. That's point one.

The second is the Court shouldn't certify a breach of contract claim under those circumstances because a favorable classwide judgment on nominal damages would preclude absent class members from pursuing claims for any actual damages under *res*

judicata.

Now, while we dispute vigorously that any class members suffered actual damages, as I mentioned before, plaintiffs allege a host of them in their complaint, including actual fraud, which they concede can't be resolved on a classwide basis and don't seek to certify for classwide treatment.

In other words, proceeding with a class claim for solely nominal damages would not be the superior method because it's inconsistent with the case that plaintiffs have brought. If the Court declines certification of plaintiffs' classwide injuries, these classwide injury theories that we've talked about, it should decline certification for the breach of contract claim altogether.

Plaintiffs' incorrect view of how nominal damages would be awarded confirms that certification of a nominal damages only claim is not the superior method of adjudication here. As we explained in our opposition brief, the Fourth Circuit has not condoned awarding nominal damages in a class action to each class member. Rather, in the *Norwood v. Bain* case that we cited, the Fourth Circuit followed the typical practice of awarding one dollar in nominal damages to the class as a whole. Similarly, other courts have

awarded nominal damages only to the named plaintiffs in cases. Virginia courts routinely describe nominal damages as, quote, token or, quote, trivial. There's nothing token or trivial about a $9.8 billion nominal damages award.

Plaintiffs have no good answer to *Norwood*. They just repeat the same Ninth Circuit case, *Cummings v. Connell*, which, in addition to being an outlier, expressly noted that its ruling was contrary to *Norwood*. Plaintiffs also fail to meaningfully engage with the authorities that we cite showing an award of $9.8 billion where no class member has suffered actual harm would violate due process.

Finally, plaintiffs complain that Capital One shouldn't be let off the hook just because we got lucky that Paige Thompson was caught before the data could be misused. But this just proves that plaintiffs are trying to use nominal damages which were meant to be a symbolic, trivial award to impose punitive damages on Capital One even in the absence of actual harm to any plaintiff.

Plaintiffs' argument does call to mind the Supreme Court's analogy in *Ramirez* that if a reckless driver exposes another motorist to a risk of harm but no accident occurs, that would ordinarily be cause for

celebration, not a lawsuit, and certainly not a lawsuit seeking $9.8 billion in nominal damages.

Two final points on nominal damages, Your Honor. Plaintiffs suggest that the Court need not decide now whether nominal damages can be awarded to each class member saying this should be determined at the damages phase of the case. But while the amount of nominal damages is properly considered later, the Court should decide the gating legal question of whether each class member can recover nominal damages because it is critical to the Rule 23 analysis.

Plaintiffs say in a footnote also that nominal damages may be available for their negligence and unjust enrichment claims. We vigorously disagree with that. But in any event, that's just further proof of plaintiffs' singular focus on obtaining class certification irrespective of whether it can result in any meaningful relief for the class. In short, class claims for solely nominal damages do not meet Rule 23 superiority requirement under the facts of this case.

That concludes my remarks on nominal damages. Unless the Court has any questions, I now want to just quickly turn to several of plaintiffs' causes of action and discuss them in a little bit more detail.

THE COURT: All right.

MR. BALSER: And specifically, I want to touch on their breach of contract, unjust enrichment, and statutory claims through the Rule 23 lens. Our arguments, again, are going to focus primarily on predominance, but I'm also going to discuss typicality and adequacy under Rule 23(a)(3) and (a)(4).

Let's start with their breach of contract claim. In short, there are three reasons that plaintiffs can't satisfy predominance as to this claim:

The first is that the relevant contractual obligations, that is, those that are contained in the privacy notice, differ across the putative class.

Second, the applicants who are not represented by this, in our view -- represented by these eights plaintiffs -- would have to present individual proof regarding contract formation.

And third, resolving contract requirements and defenses requires consideration of facts specific to each class member such that classwide relief would be inappropriate.

Plaintiffs have seized on a phrase in the privacy notice that states that Capital One's security measures comply with federal law. But because that privacy notice did not contain that language before 2010, a breach of contract claim premised on the

pre-2010 privacy notice differs significantly from a claim premised on a post-2010 privacy notice.

And it's not as simple a question as Mr. Siegel would like the Court to think about whether that's something that can just be figured out with the press of a button by Capital One. Individualized determinations would be required to determine when any particular class member applied for a credit card, which version of the privacy notice was then in effect, whether Capital One approved the application, and, if so, whether any updated version of the privacy notice, that is, for example, a version including plaintiffs' favored "comply with federal law" language applies to that putative class members' information that was stolen in the cyber incident.

Plaintiffs' primary response to this argument is that some automated review of our files would show which privacy notice applies, but that's not right. Plaintiffs overlook that many plaintiffs and class members -- I mean their named plaintiffs and additional class members -- submitted multiple different applications at different points in time. Some of which were granted, some of which were not.

If an application were granted, the Court would have to determine how long the account remained

open and if an updated post-2010 privacy notice applied to the account. The Court would then have to determine whether the information that was impacted in the cyber incident pertained to an application or an account that was governed by the pre-2010 or post-2010 version of the privacy notice, an issue that itself might be contested. In short, Capital One cannot just press a button to generate a straightforward answer to these questions.

Similar predominance issues exist with respect to the applicants only. In their opening brief, plaintiffs asserted that all applicants are provided with the privacy notice during the application process. We disproved that assertion in our response showing that some applicants were not provided with a copy of the privacy notice at the time that they applied. Other applicants had access to the privacy notice but were not required to read it, and some plaintiffs testified that they never look at privacy notices before applying for credit. Plaintiffs do not address any of this evidence in their reply brief, and they indisputably have not developed classwide evidence that applicants were presented with, read, or relied on the privacy notice.

For applicants to be able to enforce the

privacy notice, they must present evidence that that notice formed part of the bargain that they struck with Capital One.

We've cited in our brief the just black-letter law *Giordano v. Atria Assisted Living*, an Eastern District of Virginia case that says in order for a valid contract to be formed, the axiomatic meeting of the minds must occur. There can be no mutual assent where one party is not even aware of the existence of the contract.

And we cited this case from the Western District of New York that's an interesting case. It's the *Fero v. Excellus Health Plan* case. In that case, it's very similar to this issue that we're talking about now, and that case involved a health plan. Some health plan members were provided a copy of the privacy policy while others were only provided a link where they could access the document, which is the case here with respect to many of the channels. We looked at that chart earlier and the different ways people can apply. The court there held that there was no predominance because of the need for individual inquiry into whether a given class member received a paper copy of the privacy or a link thereto. That is, the court denied certification of a Rule 23(b)(3) class on the

very issue presented in this case, that is, the lack of common proof that all applicants received the privacy notice.

Plaintiffs don't dispute and, therefore, concede that many applicants were not given the privacy notice at the time of application. So if the Court agrees with us that applicants cannot enforce a contract that they didn't know existed, then it should also find that these questions of contract formation defeat predominance.

Very quickly, Your Honor, I want to mention the defenses we have to the contract claims. We've explained in our briefs why determining which class members are subject to the defenses of first material breach -- and the related doctrines of setoff and recoupment -- require individualized inquiries. Plaintiffs argue that we waived that defense by not explicitly pleading it, but we did plead setoff.

This court in the *Dowell v. G&G Motorcycles* case, which is an Eastern District of Virginia 2014 case, said that an affirmative defense may be pleaded in general terms and will be held to be sufficient as long as it gives fair notice to the nature of the defense.

In any event, Capital One can raise an

affirmative defense as to absent class members even if that defense does not apply to the named plaintiffs. That's a well-established point of law. We cited the *Gunnells v. Healthplan* case, a Fourth Circuit case from 2003, for that proposition.

And finally, plaintiffs repeat their refrain that resolving this defense merely involves automated review of Capital One's customer files, but that's not true. In fact, we don't need to look any further than the representative plaintiffs to see why automated review of Capital One's files would not resolve Capital One's first material breach defense.

If we could, just take a look at Sara Sharp. We've got a slide up that shows her circumstances. Ms. Sharp, who is one of their named plaintiffs, applied for credit from Capital One four times. Some were denied. Some were approved. She had multiple Capital One-issued credit cards. She's filed for bankruptcy twice, once in 2000 and once in 2017. She also routinely carried a balance on her Capital One account and left Capital One with nearly $1,000 in debt to charge off on at least one card.

Thus, determining whether her claims are barred by the first material breach doctrine would require analysis of whether the data of hers that was

impacted in the breach related to one of the accounts that was charged off, whether Capital One did anything that could be construed as waiving her breach, for example, by issuing her another card, whether that breach was material or partial, etc.

She's only one of the 98 million people in this putative class, but she provides a nice example of the highly individualized inquiry that would be necessary for us to be able to assert defenses available to us for this breach of contract claim. And there's just no automated review of our files that could resolve these and other similar issues for 98 million individuals.

I want to switch gears and address plaintiffs' unjust enrichment claim.

THE COURT: All right.

MR. BALSER: I want to first discuss why the plaintiffs, who are all cardholders, are neither typical or adequate to assert this claim on behalf of the applicants. Then I'll explain why the unjust enrichment claim independently fails the predominance test.

So I know Your Honor is familiar with the standards for typicality and adequacy. Rule 23(a)(3) provides the standard for typicality. The claims or

defenses of the representative parties must be typical of the claims or defenses of the class. Rule 23(a)(4) is the adequacy test. Plaintiffs must demonstrate that they will fairly and adequately protect the interest of the class. It's black-letter law that a unique defense precludes a finding of typicality because of the danger that the unique defense will preoccupy the class representative to the detriment of the interest of the absent class members.

So let's talk about typicality. Plaintiffs here fail the typicality requirement with respect to their unjust enrichment claim because they cannot assert such a claim. They don't have the claim in light of their express contracts with Capital One. The alleged class includes 33.8 million applicants, but no plaintiff is an applicant. They're all Capital One cardholders.

Plaintiffs have conceded on the record that there's no unjust enrichment claim as to plaintiffs who entered into a cardholder agreement and have express contractual rights under the privacy notice. And a long line of cases establishes that to satisfy the typicality requirement, a class representative must be part of the class and possess the same claims and injuries as the class. A class representative also

cannot be subject to a unique trial defense that would result in dismissal of the claim asserted on behalf of the class. Plaintiffs' unjust enrichment claim and implied contract claims, therefore, cannot be certified.

And there's another problem, and that's adequacy. For similar reasons, plaintiffs are inadequate to pursue the quasi-contractual claims on behalf of the applicants. As cardholders, plaintiffs are incentivized to pursue their breach of express contract claim. The applicants who would not benefit from that claim, because they don't have it, are incentivized to pursue quasi-contractual claims, such as unjust enrichment. Plaintiffs do not share those incentives because they do not have and cannot pursue an unjust enrichment claim.

For example, plaintiffs are already pressing a nominal damages express contract claim that would negate the unjust enrichment claim for what, in our view, should be, at most, a $1 recovery to the entire class.

Now, in their reply, the plaintiffs make the predictable argument that their contractual and quasi-contractual claims all rise from the same data breach and security failures; thus, Capital One's

challenges can be discarded. But that position ignores black-letter law holding that a named plaintiff must possess the same claim as absent class members and be a member of the class that he or she seeks to represent. Plaintiffs are not members of a class that can assert quasi-contractual claims, and this creates a fundamental conflict of interest.

So in addition to those threshold problems, fatal threshold issues, they fail to meet their burden of showing that they can prove their unjust enrichment claim on a classwide basis using common evidence. So this is the predominance argument.

On reply -- this is kind of amazing, and I think Your Honor touched on this this morning. In their reply brief, the plaintiffs are now trying to distance themselves from the causal basis on which their claim is premised, that is, that no class member would have applied for a Capital One credit card had they known about Capital One's allegedly deficient data security practices, such that monetary benefits should be disgorged back to the plaintiffs.

But the premise of disgorgement is to restore the *status quo ante*, and courts often look to whether the plaintiff would have acted differently absent expectation of payment in assessing unjust enrichment

claims.

And this causal connection has also been the basis for the plaintiffs' claim since the outset of the case. In their complaint -- we have this allegation up here in this chart -- plaintiffs allege that but for Capital One's willingness and commitment to maintain their data's privacy and confidentiality, that PII would not have been transferred and entrusted with Capital One.

And Gary Olsen, their expert, testified that this was the but-for world underpinning his disgorgement analysis. Plaintiffs and Olsen have simply assumed this but-for causation across the entire putative class, but they fail to show how they will be able to prove it with common evidence. In fact, they haven't even tried.

The record evidence showed that this assumption is wrong. For example, six out of the eight plaintiffs here have testified that they intended to continue using their Capital One credit cards after they learned of the cyber incident.

And this is the point, Your Honor -- this is the point I was hinting at when Your Honor asked me what the uptake on the credit monitoring was. Seven out of the eight plaintiffs did not sign up for credit

monitoring that Capital One offered after announcing the cyber incident, which undermines Olsen's assumption that data security is so important to them that it would drive their consumer behavior.

And putative class members continue to apply for Capital One cards at similar rates after the announcement of the cyber incident as they did before the cyber incident. Neither plaintiffs nor the Court can simply assume that the behavior of 98 million putative class members would be the same, especially in the face of contrary record evidence.

Plaintiffs cite no authority for their new position that they're relieved of proving the causal basis for their unjust enrichment claim. Allowing plaintiffs to ignore a fundamental premise for their claim would lead to absurd results. For example, under this new theory that they put forth in their reply brief, it would be irrelevant to them if Capital One had expressly told the putative class that it would not protect their data, if we had said it wouldn't matter to their claim as they now frame it.

In sum, plaintiffs were required to show that they will be able to prove that no class member would have applied for a Capital One card had they known about its alleged deficient data security. They didn't

conduct a conjoint analysis or put forth any other method to meet their burden. Rather, when we pointed out those problems, they ran from some of the allegations they made in their complaint and that Olsen relied on for his theory and say causation is now no longer an element.

So, for these reasons, their unjust enrichment claim can't be certified.

There's another problem with the unjust enrichment claim, and Your Honor is going to hear more about this tomorrow. But the unjust enrichment claim is also improper for class treatment in light of Capital One's statute of limitations defense. We cite *Broussard*, a Fourth Circuit case, that holds that resolution of statute of limitations defense would depend on facts peculiar to each plaintiffs' case, which defeats predominance.

We've got, I think, a nice little graphic here that illustrates the problem. In Virginia, an unjust enrichment claim must be brought within three years, but here plaintiffs seek disgorgement damages going back to 2015. To determine whether a given class members' claim is barred, the Court would have to determine, at a minimum, when that class member applied for a card, and they could have applied many times.

When Capital One migrated their application data to the AWS cloud and when Capital One used their application data to prevent fraud, if at all, plaintiffs, again, suggest this would require simple automated review of Capital One's files. But that's not so. Even assuming all application dates could be collected and analyzed for 98 million consumers spanning a 15-year period, plaintiffs do not even respond to our point that determining when a specific data element was used to prevent fraud, if at all, would be an inherently individualized inquiry.

Until Capital One used specific application data to actually prevent fraud, Capital One undisputedly obtained no benefit from having that data under plaintiffs' own theory; thus, the date on which Capital One prevented fraud using a particular data element is critical to the statute of limitations inquiry.

So, in conclusion, Your Honor, plaintiffs' failure to address individualized issues related to causation and our statute of limitations defense preclude certification for their unjust enrichment claim.

I want to talk for just one minute, literally, about other individual defenses that we've

raised. The Fourth Circuit has held that predominance may be defeated if the resolution of individual defenses depends on facts peculiar to each plaintiffs' case. That's the *Broussard* case. And even in the context of potential affirmative defenses, it's the plaintiffs who have to show that the defenses can be resolved under Rule 23 with common proof.

We explained in our brief why Capital One's defenses have limitation of liability. Failure to mitigate and contributory negligence cannot be resolved with common proof. Plaintiffs misunderstand our argument. We're not contending that any one of these defenses standing alone defeats predominance. Our point is that all of the individualized issues presented by plaintiffs' theories of injury and their substantive claims and Capital One's defenses to those claims taken together defeat predominance. The defenses raised here merely highlight the extent of individualized inquiries that would be required to adjudicate plaintiffs' claims.

We want to now turn -- and I'll do this briefly also, Your Honor -- to plaintiffs' statutory claims. And these claims under the UCL the CLRA and the GBL and the WCPA also fail under the predominance test under Rule 23. All of those claims require common

proof of causation and damages, which is lacking for the reasons we've been discussing today.

There are some complicated issues raised by those claims, and we've addressed most of them in full in our brief. But I do want to hit the key points and respond briefly to a few new arguments that the plaintiffs made for the first time in their reply brief.

To start, if you look at their initial motion, if you look at plaintiffs' opening brief, they gave very short shrift to these claims. In fact, plaintiffs did not even mention in their opening brief what injuries could support those proposed statutory claims. On that basis alone, the Court can and should decline certification because it's plaintiffs' burden to meet the requirements of Rule 23. And by clarifying those injury theories for the first time in their reply, they waive those arguments.

But had they timely asserted the injuries that they now seek to certify under the statutory claims, we would have explained how none of the plaintiffs can pursue those claims. We explain in our motion for summary judgment why the claims fail on their merits. I'm not going to get into that here.

But here's the point: The plaintiffs made

clear for the first time in their reply brief that they're relying on the market value theory and the increased risk of harm theories of injury to support their statutory claims. Those injury theories fail for the reasons we've been discussing almost all day today, meaning that the plaintiffs' statutory claims can't be certified because the damages theories under which they're traveling are not certifiable.

But even if the claims weren't doomed on the merits, plaintiffs have failed to meet their burden by showing that they can prove the claims on a classwide basis with common evidence.

It's unclear. I heard Mr. Siegel say, I think, earlier today that the plaintiffs are not relying on alleged misrepresentations by Capital One regarding the status security practice to support these claims. Their brief suggests otherwise. But whether they are or aren't or whether they're relying on purported omissions, plaintiffs can't point to any common misrepresentation or omission that all 98 million of the putative class members were exposed to before they applied for credit cards, as would be required to show causation and damages under those claims.

They also suggest that we had some duty to

disclose to the class allegedly deficient data security practices. That's a fraudulent concealment claim which plaintiffs expressly disavow that they were asserting in their motion to dismiss briefing. And they haven't pointed to any duty that Capital One had to affirmatively disclose anything to the class.

So before moving on, I just would note that the claims suffer from specific problems with respect to each of those statutes as well. The WCPA, the Washington statute that they're traveling under, permits recovery for injuries to business or property, which plaintiffs don't even assert here.

The CLRA can only apply to those class members who applied for a card for personal, family, or household purposes, and plaintiffs fail to show how they can prove that condition across the class using common evidence.

Also, the CLRA by its terms does not apply to the extension of credit. So plaintiffs would have to prove a violation of the statute with respect to an ancillary service used by each class member. Plaintiffs cannot make that showing across the class with common evidence.

Finally, plaintiffs ask the Court to certify statutory claims for injunctive relief. The Court

should reject that request for the same reason it should reject plaintiffs' request to certify a Rule 23(b)(2) class, which is what I'd like to turn to now.

Plaintiffs have failed to meet their burden of showing that certification of an injunctive relief class under Rule 23(b)(2) is warranted. As I explained in connection with our standing motion, none of the named plaintiffs has Article III standing to pursue injunctive relief against Capital One because they cannot show that they face a real and imminent risk of being harmed by another similar breach of Capital One's systems. Because no plaintiff has standing to seek injunctive relief, no Rule 23(b)(2) class can be certified.

But even if they did have standing, plaintiffs have failed to rebut all the reasons that we explained in our opposition as to why a 23(b)(2) class should not be certified here. Plaintiffs don't distinguish the Fourth Circuit case that we've cited, the *Berry* case, that holds that where monetary relief predominates, Rule 23(b)(2) certification is inappropriate.

Plaintiffs here are asking for an award of hundreds of billions of dollars. Monetary relief

clearly predominates. Plaintiffs cite a single case from the Western District of Texas permitting, so called, divided certification, but plaintiffs cite no authority suggesting the Fourth Circuit would follow that approach, nor do they explain why divided certification is warranted on the facts here.

Plaintiffs also make much of *Adkins v. Facebook* -- that's the case we talked about earlier -- where Mr. Ratner's theory of access was rejected by Judge Alsup as a basis for a negligence claim. But Judge Alsup did certify a (b)(2) class in that case.

But given plaintiffs' heavy reliance on the case, I think it's worth taking a minute to explain what happened there. To begin, the *Facebook* court denied plaintiffs' request for a (b)(3) damages class. So the rule barring injunctive relief where monetary relief predominates didn't apply. But the court also explicitly based certification of the (b)(2) injunctive class on evidence of -- and I quote -- Facebook's repetitive losses of user's privacy, closed quote.

By contrast, plaintiffs here point to a single breach, the root causes of which have already been fixed. So this Court should take a dim view of plaintiffs' heavy reliance on *Facebook*.

In their reply, the plaintiffs fail to take

on our argument that injunctive relief is unwarranted because there's no evidence of dissemination, and Capital One has already completed extensive remediation of the issues that led to the cyber incident.

They likewise fail to address our arguments that the Court can't order us to engage with criminals on the dark web, which is part of the relief they seek. And many of the measures that the plaintiffs seek, like deletion of data, are unrelated to the causes of the cyber incident.

For all of these reasons, the Court should not certify a Rule 23(b)(2) injunctive relief class.

Plaintiffs wave at an issue, a certification argument, under Rule 23. I think it's fairly obvious to the Court by now that certifying -- I mean, certifying an issue class on duty and breach alone leaves the hardest issues of causation and injury still undecided. So if the Court were to certify an issue on duty and breach and send the cases back to the 98 million people for trial, they still would have to prove causation and injury, which are the real issues, the hardest real issues to grapple with here. So even if the Court went through the trouble of resolving duty and breach on a class basis, it would still be left with 98 million individual trials on the most complex

issues we have, and that's not material advancement.

So given the complexity and difficulty in proving causation and damages, few, if any, class members would actually benefit from a ruling on duty and breach.

So, to wrap up, Your Honor, to conclude here, just a quick trip of where we've been. I've explained or tried to how all the claims that plaintiffs ask to certify are plagued with individualized issues. I've also explained, with respect to the unjust enrichment claim, that the named plaintiffs aren't typical or adequate class representatives. And I've just discussed why certification of a Rule 23(b)(2) injunctive relief class and certification of limited issues is unwarranted.

Again, it's the plaintiffs' burden to prove that they meet the requirements of Rule 23. It's not Capital One's job to disprove it. Plaintiffs have not carried their burden.

In closing, I would like to draw the Court's attention back to Rule 23(b)(3)(D)'s superiority requirement. Rule 23(b)(3)(D) provides that in determining whether a class action would be the superior method for adjudication, the Court should consider the likely difficulties in managing a class

action, and the advisory committee notes state that a critical need is to determine how the case will be tried.

I know Your Honor is a very experienced trial judge; thus, when considering plaintiffs' motion for class certification, I urge the Court to think about what a trial would actually look like in this case based on all of these individualized issues that I've outlined today.

As I mentioned earlier, the Supreme Court in *Ramirez* confirmed that in a class action, plaintiffs must factually establish with evidence each absent class member's alleged harms. The Court cannot simply presume that an absent class member suffered the harms alleged by the named plaintiffs. Plaintiffs have failed to show how they can prove the alleged harms of each of the 98 million class members in an efficient manner using common evidence. Rather, the jury would be required to preside over literally tens of millions of individual trials to prove plaintiffs' classwide injury theories.

And these individualized inquiries would include, for example, on the increased risk of harm theory, the jury would have to consider broad variation in individual class members' risk profiles and whether

the cyber incident uniformly increased the risk levels across a range of 724 different combinations of stolen data, many of which pose no risk of harm at all.

On the market value theory, the same complications would infect the trial, and Capital One would be entitled to dispute the value assigned to any given class members' stolen data, including by presenting evidence that the data was exposed in a prior breach or publically available online or the data was obsolete or inadequate.

On the disgorgement theory, evidence would have to be presented on whether any given class members' application data was used in a fraud model during the relevant time frame, whether it actually prevented any fraud, and whether that class member received any benefits in exchange for providing that PII to Capital One.

And on nominal damages, individualized inquiries would be required to prove causation and harm, even to recover just nominal damages, and to resolve the contract defenses and requirements Capital One has identified.

Plaintiffs have failed entirely to show how a trial could feasibly be conducted on these facts. It's clear it cannot be. Telling evidence of how

unmanageable a trial would be is plaintiffs' failure to submit a trial plan to the Court explaining how this case could be efficiently tried. Mr. Siegel said he's thought about one, but I haven't seen one. I don't think the Court has either. Indeed, no data breach class action has ever gone to trial and for good reason.

In closing, Your Honor, this case is not conducive to classwide resolution, and envisioning what a trial would look like proves that point. Because plaintiffs have failed to carry their burden to establish compliance with Rule 23, the Court should deny their motion for class certification in its entirety.

THE COURT: All right. Thank you.

MR. BALSER: Thank you.

THE COURT: Mr. Newby.

MR. NEWBY: May it please the Court. I will be concise here. Mr. Balser very comprehensively argued and effectively argued the reasons why this Court should not certify the class. I just want to -- and Amazon has joined in the arguments that Capital One has made both on Article III standing, as well as in its opposition to the motion for class certification.

I do want to address just a couple of gaps

that are different in both claims that are asserted against Capital One and Amazon, as well as one difference with respect to unjust enrichment.

First of all, as Mr. Siegel pointed out this morning, the plaintiffs are seeking class certification on their Florida deceptive practices claim against Amazon but not against Capital One. And the reasons why class certification is not appropriate for that claim is very similar to the arguments that Mr. Balser was making as to the other statutory claims.

First of all, the plaintiffs here have not shown standing. Under the Florida statute, plaintiff is only entitled to recover actual damages, and actual damages are fairly narrowly construed under Florida law.

We cited the *In re Brinker Data Incident Litigation* case -- that's a Middle District of Florida case -- on this proposition. That was a case that involved a breach involving credit card information for consumers at a restaurant chain, and the court there noted that unauthorized charges, lost time, and lost cash back rewards are all consequential damages, not actual damages.

And what's required to show actual damages and actual injury, standing to bring a claim under the

Florida statute, is some damage to the diminished value of the goods or services that are received by a consumer in a consumer transaction, and that's not what the plaintiffs are seeking here. They're seeking either some disgorgement, or they're seeking this lost value type remedy. They're not seeking any kind of injury related to the lost value of the credit card services that they received from Capital One.

So, in sum, they don't have standing to bring the Florida claim. They haven't alleged actual damages, and they can't prove actual damages. Certainly, they can't do so on a classwide basis.

Secondly, just one other finer point in response to Mr. Siegel's argument this morning on this omission theory that all of their state statutory claims are not really based on an actual misrepresentation but on an omission. And I agree with Mr. Balser that the complaint doesn't really read quite that way. But even to the extent that they are presenting an omission theory, individualized issues are going to predominate over common ones as to Amazon as the testimony that we obtained from the representative plaintiffs shows.

None of these plaintiffs, none of the representative plaintiffs, had any idea or any

awareness of Amazon's relationship with Capital One when they applied for or when they used their cards. None of them -- or I should said every one of them confirmed that it was not a factor. The fact that Capital One used Amazon Web Services to host and process information and to run its back-end information technology was not a factor in their decision to apply for or use a Capital One card.

And what's more, most of them -- I believe all but one -- had never even heard of Amazon Web Services before this lawsuit. Some of them hadn't heard of it until just weeks before their depositions.

So even if there were an omission that the plaintiffs could identify -- and they haven't identified one throughout the course of discovery, an omission of fact that Amazon should have made -- there's no evidence that any of the representative plaintiffs would have had exposure to that omitted statement, that they would have considered it.

And certainly, perhaps somewhere out there in the 98 million class members there could be somebody, but that's a highly individualized issue based on what they were aware of based on the information -- you know, their individualized knowledge and understanding of Amazon Web Services.

I'd like to turn to unjust enrichment. The plaintiffs do have a slightly different -- well, I should say it's more than slightly different. It's a different unjust enrichment theory as to Amazon versus Capital One.

For Capital One, they're seeking the unjust enrichment in some value that they allege Capital One received from their personal information and preventing against fraud loss.

With respect to Amazon, they're simply seeking that Amazon disgorge the entirety of the profits that Amazon earned from five years and a month of Capital One paying Amazon for providing a range of cloud services, cloud computing services. And we have addressed these claims in our motion for summary judgment, which are not before the Court right now. But two points on this theory: One is -- well, I should say three points. One is this theory is based entirely on Mr. Olsen's testimony. As we'll get through tomorrow, that testimony and that opinion is unreliable. And if that goes away, then the position is that this theory of injury falls away as well.

Secondly, the unjust enrichment theory suffers from the same Article III standing challenges and problems that Mr. Balser very comprehensively

explained earlier this afternoon. Just the mere assertion of an unjust enrichment cause of action, common-law cause of cause, even thought it's a cause of action that has been recognized at common law, the mere assertion of that cause of action is not enough in and of itself to establish standing.

This was addressed in the *Baehr v. Creig Northrop Team* case. Mr. Balser mentioned it earlier in his argument. That's a Fourth Circuit case. This is a case in which unjust enrichment was considered as a remedy for a statutory violation. And in that case, it was a violation of the Real Estate Settlement Procedures Act where the plaintiffs had alleged that the defendants had received kickbacks for doing closings of real estate. And there were no other types of actual damages that the plaintiffs could identify, but what they did say was, well, we're seeking unjust enrichment for the kickbacks that these defendants received. And the court affirmed that unjust enrichment, because it in and of itself as a cause of action does not require a plaintiff to prove injury to themselves, that is, that the defendants were unjustly enriched at the detriment of the plaintiffs, then just merely asserting that cause of action is not sufficient to establish standing.

But that's the exact problem that we're in and what Mr. Balser covered this afternoon, that the plaintiffs here have not identified how Capital One's payment over five years of fees to Amazon under their contracts to provide cloud computing services to Capital One over that period of time, how that has worked to the detriment of the plaintiffs. They haven't identified any of that because they haven't identified any injury. And for that reason, they don't have standing to bring the unjust enrichment claim.

Secondly, as Mr. Balser pointed out, in their unjust enrichment claim -- and this is paragraph 183. And I believe on the slide that Mr. Balser used these brackets for this allegation for Capital One instead of defendants. But the way that the plaintiffs have pled this case is that they would not have provided their personal information to Capital One and by extension to Amazon, but for certain promises that were made about protecting the security and privacy of their person information.

That's the way they pleaded the case. That's not the way that the evidence has come out. And as I said earlier, on the statutory causes of action, none of these plaintiffs was aware of any statements by Amazon, certainly, about the privacy and security of

their information. They weren't even aware of the company.

Just to close out on unjust enrichment, there are individualized issues that would predominate on this theory that the plaintiffs have that Amazon should disgorge all of its profits from Capital One, and the data that Capital One had stored on Amazon Web Services, the way that they've processed it, as Mr. Balser explained, is a high degree of variability here. We have 700-plus different variations of data for each plaintiff. The ways in which Capital One has used that data, the amount of data per class member, it's all going to vary substantially, and that's not something that can be addressed on a classwide basis.

So, for that reason, we support the position that Capital One has taken, that class certification is not appropriate and that the claims against Amazon are similarly not appropriate for class certification and that the plaintiffs lack standing here to assert those claims.

THE COURT: All right. Thank you.

MR. SIEGEL: Your Honor, I know you've heard a lot. If I could just have a brief few minutes to just touch on a few points. I know we have the burden, and I'd like to close it out, if I could.

THE COURT: All right. I'll tell you what I'd like to do, just so you can deliver some very well thought out focused thoughts, is to adjourn for today, meet at 9:00 tomorrow, and I'll give everybody 15 minutes to wrap up their position. Then we'll take up the balance of the motions. Given the number of motions, I'd like to allocate roughly 20 minutes per motion for each person to respond and then reply. So we've gotten into a lot of the merits, I think, already of a lot of the *Daubert* motions. So I think we'll be able to do that.

MR. SIEGEL: Thank you, Your Honor.

THE COURT: All right.

So everyone can get a good night's sleep, and we'll see you-all tomorrow morning at 9:00.

MR. BALSER: Thank you, Your Honor.

THE COURT: All right. The Court will stand in recess.

Time: 5:06 p.m.

I certify that the foregoing is a true and accurate transcription of my stenographic notes.

/s/
Rhonda F. Montgomery, CCR, RPR